Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x

Luiz Otávio Duarte

Orientador :
Prof. Dr. Adriano Mauro Cansian

Laboratório ACME! de Pesquisa em Segurança
UNESP - IBILCE

São José do Rio Preto – SP – Brasil
2003

Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x

Luiz Otávio Duarte

Projeto Final de Curso submetido ao Departamento de Ciências de Computação e Estatística do Instituto de Biociências, Letras e Ciências Exatas (IBILCE) da Universidade Estadual Paulista Júlio de Mesquita Filho, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado por:

Prof. Dr. Adriano Mauro Cansian
(Presidente)

Prof. Dr. Mario Luiz Tronco

Prof. Fábio Luiz Viana

Luiz Otávio Duarte	Prof. Dr. Adriano Mauro Cansian

UNESP – IBILCE – São José do Rio Preto
2003

AGRADECIMENTOS

"...AGRADEÇO A DEUS porque sei que ELE VIVE!"
Aparecida Silva - Andriella

Agradeço especialmente a meus pais Luiz e Solange, pelo amor, educação, credibilidade e carinho.

Ao meus irmãos José Augusto e Adriana pelo apoio e paciência despendida.

À Lívia, minha namorada, pelo amor, carinho, paciência e compreensão durante mais de três anos de namoro.

Aos meus amigos: Artur (Maguila), Denílson (Juarez), Luiz Fernando (Fefa), Marcelo (Faiskaum), Silvio (Peludão), Renato pelos anos de amizade.

Ao meu orientador Adriano, pelos ensinamentos, sugestões, críticas e conselhos.

Ao Marcelo (Faiskaum) e ao André (Ruivinho) pelos trabalhos desenvolvidos em conjunto e pelos momentos de descontração.

Ao Marcelo (Cave) e ao Artur Renato pela ajuda, amizade e companheirismo desde iniciar o estágio no laboratório.

Ao César (Burca) e Thiago (Jiló) pelas informações e ajudas trocadas nas longas madrugadas passadas.

Aos demais familiares e amigos que de uma forma ou de outra me ajudaram.

"…IT REALLY WHIPS THE LLAMA'S ASS.."

- Winamp

SUMÁRIO

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

RESUMO

A tecnologia 802.11 para redes sem fio tem sido amplamente utilizada por instituições e empresas com a finalidade de economia em infra-estrutura de cabeamento, além de prover interligação, maior mobilidade e flexibilidade para redes locais. Em contrapartida, existem algumas preocupações adicionais em segurança que são inerentes a um meio de comunicação sem fio. Visando o aumento na expertise dos pesquisadores, analistas e técnicos, este trabalho analisa as vulnerabilidades e os ataques em redes sem fio conhecidos na atualidade.

ABSTRACT

The 802.11 technology for wireless networks has been widely deployed by institutions and enterprises in order to don't spend money with cabling infra-structure, providing more intercommunication and greater mobility and flexibility to the local networks. Nevertheless, there are several additional worries about security inherent to a wireless medium. Aiming for a increasing of the expertise of the researchers, analysts and technicians, this work analises the most actual vulnerabilities and the attacks in wireless networks.

1

"No início não havia início, só havia o Irônico. Ele sempre existiu, e somente
Ele sempre existiu, nada jamais existiu além Dele.."
Alessandro de Sousa Villar – Cosmogonia Irônica

Introdução

O rápido aumento da utilização das redes sem fio 802.11x no decorrer dos últimos anos é comparado com o crescimento da Internet nas últimas décadas [ASW01]. Estas redes são cada vez mais utilizadas como um auxílio precioso para as LANs "*Local Area Networks*" [KR01] convencionais, seja por prover uma alternativa economicamente viável, seja por prover taxas de transmissão comparáveis a redes guiadas.

As redes sem fio vêm sendo cada vez mais utilizadas para prover conectividade dentro de instituições. Além de serem utilizadas para criar *links* à distância entre organizações, suas filiais e clientes. Este é um novo cenário onde pessoas mal intencionadas podem ganhar acesso à rede e comprometer os computadores da instituição, transformando-a em um ambiente potencialmente inseguro.

1.1 Motivações

Por ser uma tecnologia relativamente recente, muitas vulnerabilidades podem ser encontradas e outras ainda serão descobertas. É justamente explorando estas vulnerabilidades que atacantes se infiltram nas redes sem fio. A forma comumente utilizada para explorar estas vulnerabilidades é através do uso de ferramentas desenvolvidas especificamente para esta finalidade.

Ataques direcionados às redes sem fio além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Esta rede tornou-se um alvo fácil e almejado por pessoas mal intencionadas para o comprometimento de sistemas, pois disponibiliza inúmeros atrativos como dificuldade na identificação da origem exata do ataque, imaturidade das opções e protocolos de segurança para

esse tipo de tecnologia, facilidade em obter acesso a rede guiada através de uma conexão de rede sem fio e principalmente a falta de conhecimento técnico do gerente desta rede.

Para que os ataques dirigidos às redes sem fio possam ser identificados e as contra-medidas possam ser tomadas eficazmente, é necessário que haja a análise das vulnerabilidades inerentes às redes 802.11x. Para isso, é preciso um estudo exaustivo sobre os protocolos que dão suporte às mesmas. Com isso as falhas nestes protocolos são apontadas e as mudanças cabíveis podem ser introduzidas.

1.2 Objetivos

Este projeto estuda os protocolos que dão suporte às redes 802.11x, analisando suas vulnerabilidades, as técnicas de ataques e as ferramentas mais utilizadas por pessoas mal intencionadas para o comprometimento destas redes, tendo como objetivo fornecer a base conceitual necessária para que ferramentas de segurança para redes 802.11x possam ser desenvolvidas.

A análise das vulnerabilidades é voltada ao estudo das falhas de segurança presentes na estruturação dos protocolos 802.11x. Soma-se a esta análise, outra onde se leva em consideração a comunicação entre os dispositivos de rede sem fio.

O estudo das técnicas utilizadas para explorar estas vulnerabilidades também é realizado. Com esse estudo, são identificados o grau de conhecimento do atacante, informações de vulnerabilidades ainda não conhecidas e formas eficazes de se identificar quando algum destes ataques está sendo disparado contra determinada rede.

O projeto, portanto, analisa as vulnerabilidades, o grau de comprometimento atingido por cada uma delas, como podem ser exploradas e como podem ser eliminadas.

1.3 Organização do projeto

Este projeto é subdividido em três etapas principais. Na primeira etapa, é ilustrada a conceituação teórica necessária sobre o funcionamento de redes sem fio e seus protocolos, mais especificamente o padrão IEEE 802.11b [IEE99.], levando-se em conta também outros padrões como o IEEE 802.11g [IEE03]. Conceitos importantes como topologia, diferenciação de WLANs e *ethernet* [KR01], bem como os mecanismos de autenticação e criptografia são estudados para o completo entendimento de suas vulnerabilidades.

Na segunda etapa de desenvolvimento, testes práticos são realizados com o objetivo de validar as vulnerabilidades encontradas, além do estudo das principais ferramentas utilizadas para explorar as falhas das redes sem fio. São elaboradas simulações de ataques utilizando ambientes experimentais. Nestes experimentos máquinas são configuradas para atuarem como clientes válidos, *access points*[IEE99] e atacantes. Também é utilizado um dispositivo para captura de todo o tráfego para que as análises pertinentes possam ser realizadas.

Na terceira etapa do projeto é realizado o estudo das vulnerabilidades encontradas com a finalidade de que alternativas de segurança às redes sem fio. Visto que os resultados das análises

e dos testes práticos tornam isto possível. Nesta última fase também são incluídos resultados e conclusões sobre a segurança em redes sem fio, levando em conta as vulnerabilidades estudadas e as formas de proteção encontradas.

2

"Conheça o inimigo e a si mesmo e você obterá a vitória sem qualquer perigo...".
Sun Tzu – A arte da guerra

Fundamentação Teórica

2.1 Considerações iniciais

Neste capitulo é apresentada a fundamentação teórica necessária para o entendimento acerca do desenvolvimento deste trabalho, o qual baseia-se na análise das vulnerabilidades e dos ataques inerentes a redes sem fio 802.11x.

A pilha de protocolos TCP/IP [1], seus elementos e funcionalidades são mostrados inicialmente, bem como, as principais diferenças entre redes *ethernet* [KR01] e redes sem fio 802.11x.

Em seqüência são abordados aspectos sobre as especificações da camada de enlace de dados e da camada física das redes sem fio. São ilustrados conceitos fundamentais das redes sem fio, criptografia e autenticação e as formas de controle e gerenciamento presentes no protocolo 802.11.

Por fim, são apresentados importantes aspectos sobre segurança de computadores e redes, tomando como parâmetro principal a segurança de redes sem fio, apontando quais características são desejáveis *a priori*.

2.2 Redes de computadores e a pilha de protocolos TCP/IP

Segundo [FBA98], uma rede de computadores é um grupo de dispositivos (freqüentemente chamados de nós) interligados entre si. Estes dispositivos são geralmente *hosts*[2]

[1] TCP/IP é um agregado de regras que permitem a comunicação entre diversos dispositivos uma rede de computadores. Vide 2.2

(*end systems*), impressoras, ou qualquer outro dispositivo capaz de trocar dados com os outros nós desta rede [KR01].

A comunicação entre os diversos dispositivos da rede de computadores deve ocorrer de forma ordenada, visto que esta comunicação ocorre entre diferentes sistemas. [Ste94]

Através do uso de protocolos, que são um agrupado de regras que gerenciam a comunicação de dados, é possível interligar vários dispositivos com os sistemas mais variados. Existem alguns comitês, tabela 2.1, que se dedicam a estabelecer e manter padrões e protocolos para dados e telecomunicações.

Tabela 2.1 – Comitês criadores e mantenedores de padrões e protocolos. [FBA98]

The Internet Society (ISOC)
The International Standards Organization (OSI)
The International Telecommunications Union (ITU-T, formalmente o CCITT)
The American National Standards Institute (ANSI)
The Institute of Electrical and Electronic Engineers (IEEE)
The Electronic Industries Association (EIA)
Bellcor

É justamente através da utilização de padrões previamente definidos que se torna possível a existência da Internet. Esta é entendida como a interconexão de milhões de dispositivos computacionais ao redor do mundo [KR01].

O *Internet Engineering Task Force* (IETF) [IET03] é uma comunidade internacional de projetistas de redes, operadores, fabricantes e pesquisadores preocupados com o desenvolvimento da arquitetura da Internet. O IETF é uma atividade organizada do ISOC [ISO03] e também é responsável por manter a especificação oficial do *Internet Protocol* (IP) e do *Transmission Control Protocol* (TCP).

Uma das pilhas de protocolos mais utilizada para interconexão em redes de computadores na atualidade é conhecida como pilha TCP/IP (*Transmission Control Protocol/Internet Protocol*). Esta referencia dois dos protocolos de rede mais conhecidos e utilizados na Internet: o protocolo IP mantido sobre o RFC 791 [RFC-791] e o protocolo TCP mantido sobre o RFC 793 [RFC-793].

O estudo e entendimento do funcionamento do modelo TCP/IP é necessário neste projeto para a compreensão de algumas vulnerabilidades nas redes sem fio, para que o funcionamento das ferramentas maliciosas possa ser entendido e para que o estudo seja feito da maneira mais completa possível. Outro ponto importante que torna necessário o estudo da pilha TCP/IP é a necessidade em se diferenciar as redes sem fio das redes guiadas[3].

As principais características da pilha de protocolos TCP/IP serão apresentadas a seguir.

---

[2] *Host* ou *end system* – dispositivos computacionais como *desktops*, estações UNIX e servidores interligados em rede e que são capazes utilizar os serviços desta.

[3] Redes guiadas – redes que necessitam de cabos (fios de cobre, fibras ou outros) para interconexão dos vários dispositivos. Fazem parte destas redes: redes ADSL, redes ATM, redes *ethernet*, entre outras.

2.2.1 Pilha de protocolos TCP/IP

Tem sua organização feita em camadas, figura 2.1, sendo que cada uma destas desempenha papeis fundamentais no processo de comunicação.

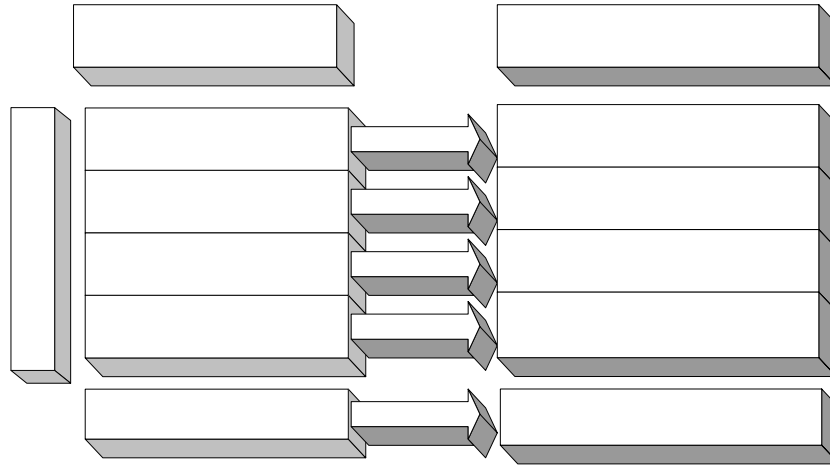



Figura 2.1 – Pilha de protocolos TCP/IP, com exemplos de protocolos de cada camada.

A comunicação nas redes sem fio ocorre através da implementação do modelo TCP/IP. Entretanto, existem algumas variações na implementação dependendo da tecnologia utilizada que serão apresentadas no item 2.3.

2.2.2 Papel de cada camada

Como dito anteriormente, cada uma destas camadas desempenha um conjunto de funções cruciais para que a comunicação ocorra.

- **Física:** A camada física coordena as funções requeridas para transmitir um conjunto de *bits* através do meio físico. Em redes sem fio este meio pode ser o ar, infravermelho ou laser. Esta camada também é responsável pelas especificações mecânicas e elétricas, como conectores, cabos, sinalização que fisicamente liga dois nós em uma rede.

- **Enlace:** Esta camada é responsável por entregar as unidades de dados (grupos de bits) de uma estação até a outra sem erros. Esta camada aceita dados da camada de rede e adiciona os cabeçalhos necessários para que o *frame* possa ser enviado para o próximo dispositivo do trajeto entre emissor e receptor.

- **Rede:** Esta camada é responsável pela entrega de datagramas através de vários *links* da rede. A camada de rede garante que cada datagrama saia de seu *host* de origem para o seu *host* de destino de maneira eficiente.

- **Transporte:** Esta camada tem a responsabilidade da entrega de toda mensagem de um *host* de origem a um *host* de destino. Também faz parte desta camada o estabelecimento, gerenciamento e sincronismo das conexões entre *host* origem e *host* destino.

- **Aplicação:** Esta camada permite *softwares* acessarem a rede. Esta provê interface com o usuário e suporte a vários tipos de serviços como correio eletrônico, acesso remoto a arquivos, entre outros.

2.2.3 Comunicação em redes TCP/IP

Para melhor exemplificar o funcionamento de uma rede TCP/IP é importante entender como a informação flui entre os diversos dispositivos que a configuram. A forma como as mensagens são trocadas, figura 2.2, no modelo TCP/IP é idêntica à maneira como esta troca é efetuada nas redes sem fio.

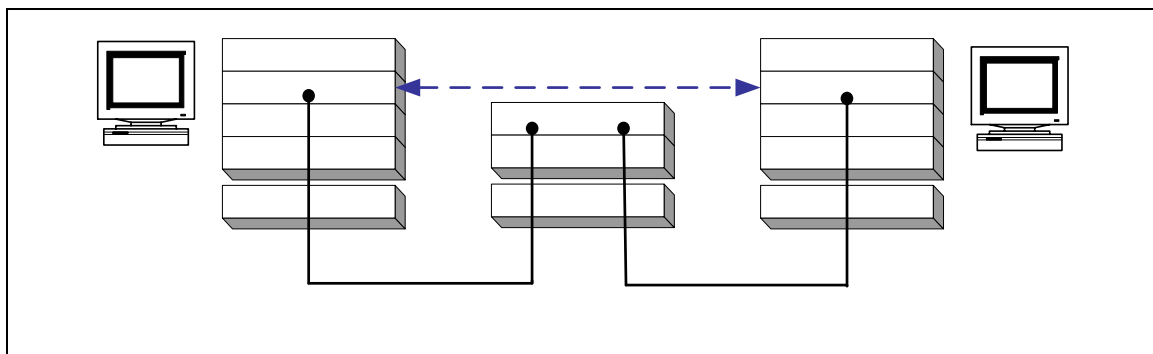



Figura 2.2 – Comunicação via pilha TCP/IP

A forma de comunicação padrão entre dois *hosts* A e B em uma rede TCP/IP faz com que os pacotes trocados apenas sejam tratados na camada de transporte e de aplicação pelos *hosts* A e B. Os dispositivos intermediários, que são compreendidos por outros *hosts* ou dispositivos de interconexão de redes, a princípio não tratam o pacote além da camada de rede da pilha de protocolos. Como será visto adiante os *access points* tradicionais atuam apenas nas três primeiras camadas: física, de enlace de dados e de rede.

2.3 Diferenciação entre redes *ethernet* e redes sem fio.

Sistemas de segurança em redes de computadores como os SDIs (Sistemas detectores de Intrusão) [Sou02], *firewalls* [ZCC00] e *VPNs*[4] [FER98], endereçam redes de computadores comumente conhecidas. Entretanto, os diferentes tipos de redes de computadores necessitam de diferentes ferramentas para segurança. Algumas ferramentas podem ser utilizadas para propósitos comuns, já outras são desenvolvidas para um único tipo específico de rede.

Por esses motivos é importante entender quais as principais modificações inseridas pelas redes sem fio em relação a uma rede convencional.

[4] (*Virtual Private Network* – Rede Virtual Privada)

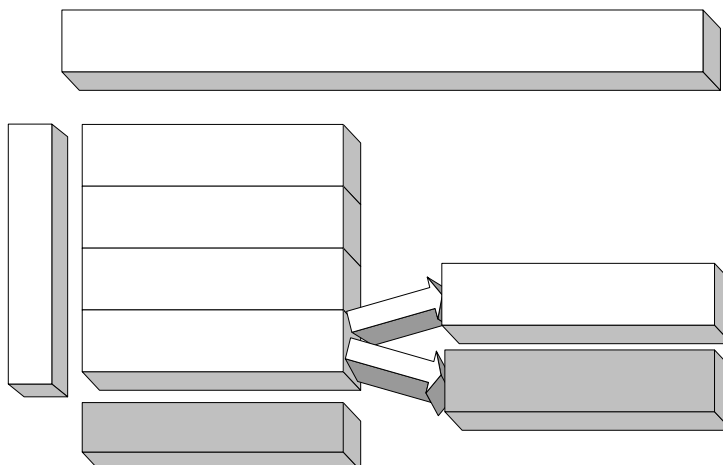



Figura 2.3 – Modificações entre redes *ethernet* e redes sem fio.

As modificações encontradas entre as redes *ethernet* e sem fio estão localizadas na camada física e na metade inferior da camada de enlace. Estas modificações são inseridas por causa da mudança do meio físico da rede e também para suportar a autenticação, associação e privacidade de estações. Com isso, a maior parte dos ataques que utilizam as camadas mais superiores da pilha TCP/IP pode ser identificada com métodos convencionais de identificação de intrusão.

Alguns SDIs que são utilizados para identificar intrusão da camada de enlace de dados precisam ser modificados para suportar esta nova tecnologia. Outros SDIs já possuem o suporte ao *linktype* das redes sem fio, mas não identificam ataque inerentes a estas redes, somente conseguem interpretar os pacotes.

2.4 Nomenclatura de componentes de redes sem fio

Por ser uma tecnologia recente, redes sem fio agregaram novas nomenclaturas que devem ser compreendidas para o estudo desta.

As redes sem fio são implementadas com dois tipos básicos de componentes. São eles, os adaptadores de redes que são interfaces eletrônicas nos computadores dos clientes e os *access points* que provêem os serviços às estações associadas.

Os *access points* são, portanto, qualquer dispositivo que faça o gerenciamento da rede sem fio. Ele pode atuar ainda como um *bridge* [KR01] entre a rede sem fio e a rede guiada.

Outro conceito muito utilizado para redes sem fio é o conceito de WLANs (*Wireless Local Area Networks*) que nada mais são do que redes locais sem fio. STAs (*stations*) são quaisquer dispositivos de rede sem fio que não um *access point*, cliente de uma WLAN.

Basic Service Set (BSS) é um conjunto de estações controladas por um único *access point.*

Independent Basic Service Set (IBSS) é a composição de uma rede sem fio onde as estações comunicam-se mutuamente sem a necessidade de um *access point.* Estas redes são conhecidas por *ad-hoc.*

Extended Service Set (ESS) é um conjunto de um ou mais BSSs interconectados, integrado as redes locais. Estes aparentam ser um único BSS para a camada de enlace de dados de qualquer estação associada a qualquer BSS.

Outras nomenclaturas são apresentadas no decorrer do projeto e são explicadas na medida em que ocorrem.

2.5 Padrões para redes sem fio

Quando se discute a configuração de uma WLAN existem alguns padrões (desenvolvidos ou em desenvolvimento) que devem ser considerados:

- **IEEE 802.11** [IEE97]: é o primeiro padrão firmado para redes sem fio. Apresenta suporte a WEP[5] e a implementação do sistema de rádio na banda ISM (*Industrial Scientifical Medical*) de 900 MHz.

- **IEEE 802.11a** [IEE99a]: é o padrão que descreve as especificações da camada de enlace lógico e física para redes sem fio que atuam no ISM de 5GHz. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta freqüência.

- **IEEE 802.11b** [IEE99b]: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP. Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.

- **IEEE 802.11g** [IEE03a][IEE03b]: descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps.

- **IEEE 802.11i** [WiF03]: trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e a 802.11g.

- **WPA** [WPA02]: *Wi-Fi Protected Access*: é uma nova especificação da *Wi-Fi Alliance*[6]. É baseada em torno de um subconjunto do padrão emergente IEEE 802.11i sendo desenhada para ser compatível com o mesmo, quando ele se tornar ratificado. Este padrão implementa o TKIP (T*emporal Key Integrity*)[7] e tem como objetivo ser implementado em todos os dispositivos já concebidos através do *update* do *firmware*.

[5] WEP – (*Wired Equivalent Privacy*). É o algoritmo que provê privacidade, autenticação e criptografia em rede sem fio. Discutido em 2.7.2.

[6] *Wi-Fi Alliance* [WiF03] é uma associação internacional sem fins lucrativos, formada em 1999 para certificar a interoperabilidade de produtos de redes locais sem fio, baseadas na especificação 802.11.

[7] TKIP – faz parte do padrão de criptografia 802.11i, sendo referenciado como a próxima geração do WEP. TKIP prove a troca de chaves WEP por pacote e um sistema de checagem de integridade das mensagens e um mecanismo de re-chaveamento.

2.6 Especificações da camada MAC e PHY de redes sem fio

2.6.1. Especificações da camada física

As redes sem fio utilizam-se de meios físicos alternativos às redes guiadas. Por este motivo a maneira como os dados são codificados, para que sejam injetados na rede, é diferente. Isso faz com que novos modelos para a camada física da rede sejam desenvolvidos.

Redes que utilizam o ar como meio físico possuem a especificação de *Frequency-Hopping spread spectrum* (FHSS) ou *Direct sequence spread spectrum* (DSSS). Estas são firmadas no protocolo IEEE 802.11.

A transmissão realizada através de *IrDA* (*Infrared* - Infravermelho) também é especificada no protocolo IEEE 802.11. Informações adicionais sobre as especificações da camada física podem ser encontradas em [IEE97] e [IEE99].

2.6.2 Introdução dos serviços da camada MAC

- **Serviço de dados assíncronos (*Asynchronous data service*):** Este serviço suporta que entidades da rede tenham a habilidade de trocar os chamados MAC *service data units* (MSDUs)[8] [IEE99b]. Como a transmissão é realizada sobre uma base de melhor-esforço [KR01], não existem garantias que um MSDU será entregue com sucesso.

- **Serviços de segurança:** A segurança nas redes sem fio é provida pelo mecanismo WEP [IEE99b]. O escopo da segurança é limitada à troca de informações entre duas estações. A privacidade é mantida no protocolo através da criptografia dos MSDU.

- **Serviços de ordenação:** A camada MAC não reordena intencionalmente os MSDUs exceto quando é necessário para que seja possível aumentar a probabilidade de que a entrega seja feita com sucesso, baseado no modo de gerenciamento de energia (*power management*) que foi proposto para as estações. [IEE99b]

2.6.3 Formato dos *frames* do 802.11

O formato dos *frames* utilizados nas redes 802.11x difere-se dos *frames* de outros tipos de redes. Estas modificações e inovações podem acarretar problemas de segurança dentro destas redes.

---

[8] Dados da camada de enlace de dados lógicos e que serão enviados à rede.

2.6.3.1 Formato geral de um *frame* 802.11:

Cada *frame* consiste de três componentes básicos, figura 2.4. Um cabeçalho MAC (*MAC header*) que inclui informações sobre o *frame control* (*frame* de controle)*, duration* (duração)*, address* (endereço) e *sequence control* (controle de seqüência). Outro componente incluso é o *frame body* (corpo do *frame*), o qual representa as informações carregadas por cada tipo específico de *frame*, além do FCS (*frame check sequence* – seqüência de checagem do frame), que contém um código de redundância cíclica (CRC) [KR01].

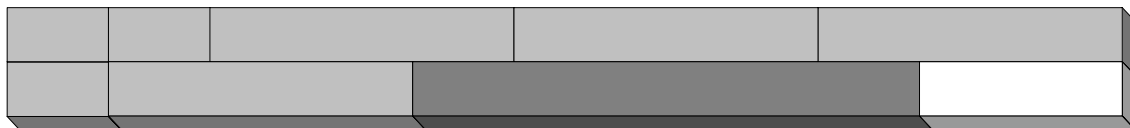



Figura 2.4 – formato geral de um *frame* 802.11

O primeiro campo é o *Frame Control*, com vários subcampos que visam à especificação das diversas características do *frame* a ser enviado.

O campo *Duration/ID* (Duração/ID), cujo comprimento é 16 bits, carrega a ID de associação da estação que transmitiu o quadro, além do valor de duração definido para cada tipo de *frame*.

Os quatro campos de *Address* (Endereço), usados para indicar o BSSID, são os endereços de origem e de destino, os endereços da estação transmissora e da receptora. Contêm 48 bits para cada endereço e podem ser de dois tipos: endereço individual ou de grupo, sendo este último subdividido em endereço de grupo *multicast* ou *broadcast*.

O campo de *Sequence Control* (Controle de Seqüência) é utilizado na manutenção dos *frames* em fluxo, possui 16 bits de comprimento e consiste dos subcampos *Sequence Number* (Número de Seqüência), de 12 bits e *Fragment Number* (Número do Fragmento), de 4 bits. Ambos permanecem constantes em caso de retransmissão.

O campo *Frame Body* (Corpo do Quadro) é de comprimento variável (0 a 2312 octetos) e contém informações acerca do tipo e subtipo dos *frame*s, além dos dados enviados e/ou recebidos.

Por fim, tem-se o campo *FCS – Frame Check Sequence*, com 32 bits, que utiliza o CRC de 32 bits para detectar erros nos *frame*s, assim que eles chegam.

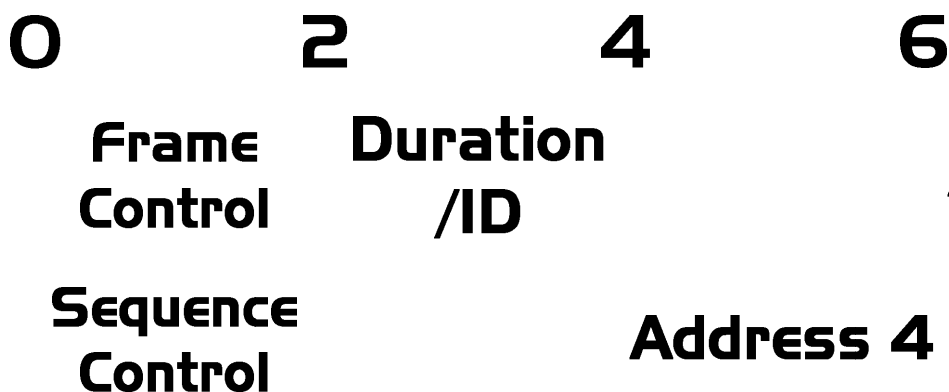
0 2 4 6

Frame Control

Duration /ID

A

Sequence Control

Address 4

2.6.3.2 Campo *Frame Control*

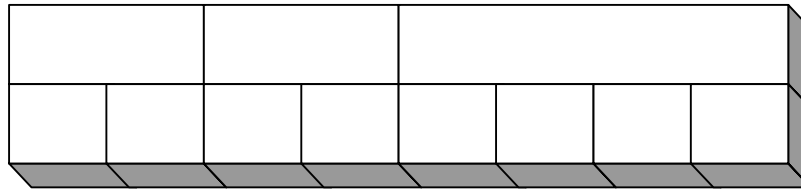



Figura 2.5 – formato do campo *frame control*.

O campo *Frame Control* consiste dos seguintes subcampos:

- *Protocol Version* (Versão do Protocolo), com tamanho fixo de 2 bits e possui valor 0 (zero) para o padrão corrente;

- *Type* (Tipo), com comprimento de 2 bits, identifica a função do *frame* e pode ser de controle, de dado ou de gerenciamento;

- *Subtype* (Subtipo), com comprimento de 4 bits, identifica a função do *frame* em conjunto com o tipo, podendo haver diversas combinações entre os mesmos;

Tabela 2.2 – Algumas combinações válidas de tipo e subtipo.

Type value b3 b2	Type Description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1011	Authentication
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment(ACK)
10	Data	0000	Data

- *To DS*[9] e *From DS*, cada qual sendo de 1 bit e tendo a função de identificar se o *frame* está sendo enviado, se está chegando, se a comunicação é entre dois *access points* ou estações;

- *More Fragments* (Mais Fragmentos), com tamanho de 1 bit, contendo valor um ou zero, de forma a indicar a existência de mais fragmentos ou não;

- *Retry* (Nova Tentativa), de comprimento de 1 bit, serve para controle de retransmissões e *frames* duplicados;

[9] DS (*Distribution System*) – É um sistema utilizado para integrar um conjunto de BSSs e integrar a rede local.

- *Power Management* (Gerenciamento de Energia), que indica o modo de gerenciamento de energia de uma estação, sendo que o valor designado um significa que esta estará em modo de economia de energia e zero em modo ativo. Seu comprimento é de 1 bit;

- *More Data* (Mais Dados), com tamanho de 1 bit, usado para indicar a existência de unidades de dados em registro no *access point* para a estação;

- WEP [IEE99b], que diz respeito a se o campo *Frame Body* contém ou não (um ou zero) informações processadas pelo algoritmo criptográfico WEP, sendo também de 1 bit de comprimento;

- *Order* (Ordem), de 1 bit de comprimento, utilizado para classificar se o fragmento usa a classe de serviço *StrictlyOrdered* (estritamente ordenado) ou não.

2.6.3.3 Campo de controle de seqüência

Figura 2.6 – Campo de controle de seqüência

O campo *Sequence Number* (Número de Seqüência) é um campo de 12 bits e indica o número de seqüência de um MSDU enviado por uma estação. Este número é atribuído pelo módulo de 4096, começando em 0 e sendo incrementado de 1 a cada MSDU.

O campo *Fragment Number* (Número do Fragmento) é o campo que indica o número de cada fragmento de um MSDU enviado. Este campo é atribuído com 0 no último ou único fragmento e é acrescido de 1 para cada um dos fragmentos remanescentes.

2.7 Criptografia e Autenticidade em redes sem fio

Existem duas abordagens recomendadas para autenticação dentro de WLANs. Objetivamente trata-se de realizar a autenticação ou na camada de enlace de dados, ou na camada de rede. A autenticação na camada de enlace é realizada através do uso de WEP. Já a autenticação na camada de rede pode ser realizada através da combinação do uso do protocolo IEEE 802.1x [MA02], que prove a autenticação tanto da estação como da entidade autenticadora.

2.7.1 Formas de autenticação em *access points.*

Quando se configura um *access point* existem três opções que podem ser usadas para autenticação. São elas:

- **Autenticação Aberta (*Open Authentication*)**: Onde qualquer estação pode se associar ao *access point* e obter acesso à rede.

- **Autenticação Compartilhada (*Shared Authentication*)**: Onde chaves WEP são previamente compartilhadas e estas são usadas para autenticar o cliente junto ao *access point*. Entretanto, se um dispositivo cliente for furtado, então todas as chaves compartilhadas serão comprometidas e precisarão ser trocadas. [ASW01]

- **Rede-EAP (*Network-EAP*)** [BV98]: Existem vários algoritmos EAP (*Extensible Authorization Protocol*). Estes protocolos dão suporte a autenticação através de servidores Radius.

2.7.2 WEP (Wired Equivalent Privacity)

Nas redes 802.11 o tráfego é criptografado através da utilização do algoritmo WEP (*Wired Equivalent Privacy*) [IEE99] [KR02]. O algoritmo é simétrico uma vez que usa chaves compartilhadas. As chaves criptográficas, chamadas de chaves WEP, devem ser as mesmas no cliente e no *access point*.

O WEP é baseado em um processo criptográfico RC4 [PF02]. Ele emprega uma chave secreta de 40 ou 104 bits que é compartilhada entre os clientes e o *access point* da rede. Durante a transmissão do pacote um vetor de inicialização (IV - *Initialization Vector*) de 24 bits é escolhido randomicamente e é anexado ao a chave WEP para formar a chave de 64 ou 128 bits. [SSK01].

2.7.2.1 Problemas bem documentados do WEP.

Atualmente os *access points* de muitas redes utilizam uma simples chave WEP que é compartilhada para todos os clientes. Com isso, a integridade e o sigilo desta chave global são quase impossíveis de serem gerenciadas.

A chave na realidade não consegue ser mantida em segredo. Como esta chave deve ser programada em todos os dispositivos autorizados é praticamente impraticável para redes com muitos clientes. Outro ponto importante é a mudança desta chave. Caso necessário isso acarretaria a modificação em todos os clientes.

Como dito anteriormente, qualquer dispositivo subtraído coloca em risco a chave WEP global o que torna o ambiente potencialmente inseguro.

Entretanto, o maior problema com o WEP é a forma como é concebido e utilizado. Desde que foi proposto, o algoritmo foi estudado e inúmeras vulnerabilidades na implementação foram encontradas. A mais conhecida é relacionada a determinados valores do IV que quando utilizados podem fazer com que a chave WEP seja facilmente identificadas [KR02]. Já chaves com valores do IV arbitrários podem demorar algumas dezenas de minutos a mais para serem quebradas.

Outro fator decisivo é que apesar de propor a "autenticação" e privacidade, este algoritmo não provê de forma efetiva a autenticação de dispositivos. Já que não suporta autenticação mútua, pois o *access point* não é autenticado pelo cliente e a autenticação do cliente

não consegue distinguir dois *hosts* diferentes.

Entretanto, esforços do comitê do IEEE 802.11 e do *Wi-fi* estudam formas alternativas, como o IEEE 802.11i e o WPA.

2.8 Gerenciamento e controle de redes sem fio 802.11x

2.8.1 Configurações de redes sem fio

Existem três formas de configurações de uma WLAN:

- **Modo *Ad Hoc*** [WH02] [VM02], onde existem somente estações sem fio que se comunicam mutuamente, sem a presença de *access points*. Todas as estações possuem o mesmo BSSID (*Basic Sevice Set Identifier*) que corresponde ao identificador da célula sem fio. O termo próprio do 802.11 para esta rede é IBSS (*Independent Basic Service Set*). Este tipo de configuração pode ser comparada a conexões *peer-to-peer* em redes cabeadas.

- **Modo de infra-estrutura básica** [VM02], onde as estações sem fio se comunicam com um simples AP. Este *access point* pode funcionar como um *bridge* entre a rede sem fio e a rede guiada. O termo utilizado para este tipo de rede é BSS (*Basic Service Set*).

- **Modo infra-estruturado** [WH02][VM02], onde redes distintas (com BSSIDs diferentes em cada uma) se comunicam através de APs criando uma única rede. Este modo tem como objetivo fazer com que o usuário possa mudar seu ponto de acesso e mesmo assim permanecer conectado. O termo mais utilizado para este modo de rede é ESS (*Extended Service Set*).

2.8.2 Associação de estações

Em redes guiadas, é necessário que uma estação esteja fisicamente ligada a outro dispositivo desta rede para poder se conectar a esta rede. Em redes sem fio, é necessário que a estação saiba qual o SSID (*Service Set Identifier* – Identificador do domínio de serviço) para poder se conectar.

Existem várias formas de um cliente saber o SSID da rede na qual vai se conectar. Uma destas formas é a configuração manual de todos os dispositivos que podem se conectar na rede. Esta forma não é muito utilizada, pois a simples mudança de um SSID acarretaria na modificação das configurações dos dispositivos autorizados.

As outras técnicas para obtenção do identificador utilizam-se de uma das duas técnicas de conhecidas de sondagem.

- **Sondagem ativa** [WJ02]**:** Feita por *softwares* que enviam *frames* de requisição em todos os canais. Os *access points* configurados de maneira a responder a este tipo de requisição o faz, sinalizando sua existência e seu SSID. Este método de sondagem é utilizado por sistemas

operacionais como *Linux*, *Unix* e *Windows*. Entretanto, alguns *softwares* maliciosos também utilizam este método.

➲ **Sondagem passiva** [WJ02]**:** Ao contrário do anterior, a sondagem passiva, também conhecido por monitoramento por rádio freqüência (RFMON), não insere pacotes na rede. A aplicação que utiliza este tipo de monitoramento captura todos os sinais de rádio freqüência no canal em que a placa de rede sem fio esta configurada para escutar. E com a devida filtragem no trafego capturado o SSID pode ser obtido.

A má configuração de *access points* faz com que a princípio este envie em *broadcast* qual é o seu SSID. A descoberta das WLANs através de *softwares* maliciosos como NetStumbler (*http://www.netstumbler.com*), DStumbler (*http://www.dachb0den.com*), Wellenreiter (*http://packetstormsecurity.nl*) e outros, que se utilizam dos métodos de sondagem descritos, é uma técnica cada vez mais popular de penetração de rede.

2.9 Riscos de segurança em redes sem fio

As redes sem fio tornaram-se alvo de exaustivos estudos e muitos ataques foram desenvolvidos e/ou adaptados para poderem se valer das fraquezas presentes nestas redes. Além disso, estas redes apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio protocolo.

A ISO define [ISO89] a segurança como a tentativa de se minimizar as vulnerabilidades de valores e recursos dos sistemas. Entende-se por vulnerabilidade as falhas ou falta de segurança das quais pessoas mal intencionadas podem se valer para invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais. Além de poder comprometer, corromper e inutilizar o sistema.

A pesquisa a cerca da segurança das redes sem fio de computadores leva em consideração quatros aspectos fundamentais:

➲ Confidencialidade: objetiva prevenir a obtenção de informação não autorizada;
➲ Disponibilidade: objetiva prevenir que recursos ou informações fiquem indisponíveis;
➲ Integridade: objetiva prevenir que mudanças ocorram em informações sem autorização;
➲ Usabilidade: objetiva prevenir que um serviço tenha sua utilidade deteriorada devido a segurança.

Estas características devem ser balanceadas para que o sistema não fique tão seguro aponto de usuários legítimos não conseguirem utilizá-lo eficientemente, e que este sistema também não seja inseguro a ponto de permitir a ação de usuários não autorizados.

Um fator importante relacionado à segurança de redes sem fio é o fato de que os ataques gerados dentro destas redes são disparados dentro do mesmo domínio de colisão. Ou seja, o atacante se comunica com o mesmo concentrador de tráfego do sistema o qual almeja atacar. Ataques como *Man-in-the-Middle* [Air00], *ARP Poisoning*[FD02], *MAC Spoofing* e outros que se valem desta posição avantajada podem ser disparados e comprometer o sistema.

Existem peculiaridades nos ataques inerentes às redes sem fio. Uma destas é o fato da utilização de equipamento próprio por parte de atacante. Ou seja, há a necessidade de que o atacante esteja dentro da área de cobertura da rede sem fio em questão e que esteja utilizando seu próprio equipamento. Os ataques convencionais em redes guiadas podem ser disparados de outros sistemas anteriormente atacados, não existindo esta necessidade.

Entretanto, o fato do atacante dispor de recursos próprios para gerar o ataque e estar próximo ao sistema que será atacado ajuda no processo de estudo e análise o conhecimento do atacante. Ou seja, projetos podem ser desenvolvidos com a finalidade de analisar o conhecimento de um atacante em dada região geográfica.

2.10 Considerações Finais

Com o que foi apresentado neste capítulo, é possível entender como as redes sem fio são implementadas e como os protocolos de comunicação atuam nestas redes. Também são apresentadas as diferenças entres as redes convencionais e as sem fio, para que se possa entender quais ataques são realmente inerentes a redes sem fio.

Com a apresentação dos campos dos protocolos das camadas inferiores do protocolo TCP/IP é possível entender quais serão os campos que possuem falhas na implementação, ou vulnerabilidades. Tendo em vista que o entendimento destes protocolos facilita o entendimento da associação, autenticação e outras funções de gerenciamento das redes 802.11.

Além do conhecimento sobre os protocolos, uma abordagem sucinta sobre criptografia e autenticação, gerenciamento e controle é realizada para o entendimento a cerca do funcionamento de uma rede real e das possíveis opções de segurança inseridas nos protocolos.

Além disso, são incluídos os conceitos de segurança para redes sem fio, baseado em conceitos de segurança para redes convencionais.

3

"Nós trabalhamos no escuro. Fazemos o possível para combater o mal, que do contrário nos destruiria. Mas se o caráter de um homem é seu destino, a luta não é uma escolha, mas uma vocação."
Fox Mulder – *Grotesque*

Desenvolvimento

3.1 Considerações iniciais

Este capítulo trata dos ataques, bem como das vulnerabilidades existentes no protocolo 802.11. Neste, inicialmente serão apresentadas as características do protocolo que podem causar algum tipo de vulnerabilidade. Estas serão abordadas mesmo que ainda não existam técnicas para explorá-las. Isto, pois estas podem representar riscos futuros à segurança nas redes sem fio.

Em seguidas são analisados os riscos inerentes das redes sem fio, sendo que estes são classificados em riscos externos e riscos internos. Estes riscos também são vulnerabilidades que podem ser exploradas através do uso de ferramentas específicas que também serão analisadas.

Neste capítulo, também é apresentado o ambiente experimental utilizado para validar alguns ataques e algumas vulnerabilidades. Por ter outros objetivos, que não a produção de *exploits* [10] , os experimentos são realizados utilizando-se *softwares* já desenvolvidos para comprometimento de redes sem fio.

Tem-se por objetivo, portanto, ilustrar as vulnerabilidades encontradas através dos exaustivos estudos realizados, mostrando como estas podem introduzir riscos à segurança de redes sem fio e como estas podem ser de fato exploradas. Além de mostrar o ambiente experimental utilizado.

---

[10] *Exploit* – São programas concebidos para explorar determinada vulnerabilidade ou sistema. Geralmente progamado por um *hacke*r experiente para ser utilizado por pessoas com menos conhecimento.

3.2 Análise das vulnerabilidades das redes sem fio

As análises baseiam-se no protocolo das redes sem fio e nas possíveis configurações dos dispositivos. As vulnerabilidades encontradas são então agrupadas em dois grandes grupos, os riscos internos e externos.

A classificação quanto aos riscos é realizada para o entendimento dos ataques e como estes podem ser identificados e minimizados.

3.2.1 Pontos vulneráveis no protocolo

O protocolo 802.11 em si é bem conciso e insere inúmeras novidades. Por ser um protocolo devidamente estudado, não possui um grande número de vulnerabilidades. Entretanto, as poucas que possui pode trazer grandes problemas à rede como um todo.

Uma vulnerabilidade em evidência hoje diz respeito à criptografia WEP. Apesar utilizar o algoritmo RC4 PRNG da RSA Data Security, INC.[11]

Outra vulnerabilidade encontrada, além de pacotes *beacon frames* com características peculiares, trata-se das formas de autenticação permitidas no protocolo.

3.2.2 Vulnerabilidades do WEP

O protocolo WEP, já discutido anteriormente no capítulo 2, é incorporado como uma parte do 802.11b. A implementação do protocolo WEP, que utiliza-se da criptografia RC4, possui algumas vulnerabilidades. Devidas à forma de implementação utilizada.

➲ **Funcionamento do RC4 no WEP**

A criptografia RC4 é simétrica, ou seja, a mesma chave utilizada para a criptografia também é utilizada para a decriptografia. Além disso, este padrão criptográfico utiliza uma cifra conhecida como *Stream Cipher* que faz com que cada mensagem seja criptografada com uma chave diferente. Isto é possível, pois é inserido um elemento adicional à chave criptográfica.

Quanto uma mensagem é passada pelo algoritmo RC4, existem duas porções de informação que são inseridas no processo de criptografia. Uma é a palavra chave e a outra é um valor randômico conhecido como vetor de iniciação (IV). Este vetor que da a característica de *Stream Cipher* ao algoritmo.

O grande problema da implementação deste algoritmo nas redes sem fio é o tamanho utilizado tanto para as chaves criptográficas quanto para o vetor de iniciação. Este apresenta uma vulnerabilidade conhecida como colisão de vetor de iniciação.

---

[11] Maiores informações sobre o algoritmo RC4 podem ser obtidas na própria RSA. Para detalhes de como se comunicar com a RSA contacte o *IEEE Standards Departament of Intelectual Property Rights Administrator* em http://www.ieee.org

O protocolo WEP utiliza 40 ou 104 bits[12] para a palavra chave e 24 bits para o vetor de iniciação. Perfazendo um total de 64 ou 128 bits. Com isso teríamos uma chave de 5 ou 13 caracteres para a palavra secreta e 3 caracteres para o vetor de iniciação.

Com 24 bits o vetor de iniciação pode possuir 2^{24} ou 16.777.216 números diferentes, os quais são escolhidos aleatoriamente. Em tese a probabilidade de se encontrar uma mensagem criptografada com o mesmo IV é de uma em 16.777.216. No entanto, por ser um número randomicamente gerado, na prática é possível encontrar uma colisão de IV em aproximadamente 5.000 pacotes trocados. O que corresponde a um tráfego de 7 a 10 MB. [PF02]

É provado que a partir de uma colisão de IV, levando-se em conta características mantidas de um pacote a outro. É perfeitamente cabível um ataque por análise de freqüência [PF02].

Como será ilustrado adiante já existem programas capazes de explorar esta vulnerabilidade.

3.2.3 Vulnerabilidades nas formas de autenticação

Os *access points* como mostrado no capítulo anterior, podem permitir a autenticação aberta. Este tipo de autenticação permite que qualquer dispositivo que saiba qual o SSID da WLAN em questão possa se associar.

Apesar de garantir a facilidade de conexão entre um cliente e um *access point*, esta forma de autenticação faz com que seja feito o *broadcast* da conexão guiada na rede sem fio. Em outras palavras, seria como colocar um *hub* em um local público, onde qualquer pessoa pode se conectar livremente.

Além disso, a forma de autenticação provida no caso de autenticação por chave compartilhada, não suporta autenticação mútua. Visto que a autenticação no protocolo ocorre através das chaves WEP. Que são únicas para todos os clientes e não autenticam os *access points*.

3.2.4 *Beacon Frames*

Devidamente especificado no protocolo 802.11. Um *beacon frame* é um frame de sinalização e sincronismo, além de enviar informações importantes a respeito do funcionamento da rede sem fio em questão.

Access points a princípio são configurados de maneira a enviar *beacon frames* no canal em que atuam, bem como no canal subseqüente e antecessor. Um exemplo de *beacon frame* pode ser observado no anexo A.

---

12 Apesar de não ser explicitamente especificada no padrão 802.11b, a criptografia de 104 bits é utilizada na grande maioria dos dispositivos.

A presença destes pacotes pode indicar que *rogue access points* [Air00] estejam ligados à rede. Estes *access points* são instalados sem a autorização e na maioria das vezes representa um grande risco de segurança a rede da instituição.

3.3 Riscos Internos

Neste primeiro grupo são incluídas as vulnerabilidades das redes sem fio que ocorrem devido à má configuração de dispositivos, configurações inseguras e associação acidental. Nos riscos internos não ocorre a ação direta de um atacante para expor a vulnerabilidade.

3.3.1 Rogue WLANs

Chamadas de WLANs grampeáveis, são instaladas na maioria das vezes sem o consentimento da instituição, portanto não seguindo a política de segurança.

Além disso, estas costumam ser instaladas por pessoas sem a capacidade técnica necessária para configurar os dispositivos. Fazendo com que estes enviem seu SSID em *broadcast*, não utilizam criptografia WEP e não levam em conta a área de cobertura da instituição, podendo assim expor esta rede a ataques advindos de locais externos a esta.

De acordo com a Gartner (*http://www.gartner.com*) em 2001 pelo menos 20 por cento das empresas possuíam WLANs grampeáveis. Estas redes podem ser facilmente escondidas da rede guiada com a duplicação do endereço MAC da máquina anteriormente ligada àquele ponto. Conseguindo desta forma transpassar *firewalls* que fazem filtragem por endereçamento MAC.

3.3.2 Configurações Inseguras

Muitas instituição aumentam o nível de segurança de suas WLANs com a utilização de VPNs e erroneamente acreditam que esta se torna à prova de invasões. Deixando de lado as configurações de segurança dos dispositivos da rede sem fio.

Entretanto, um hacker mais experiente, ao invés de tentar quebrar a VPN, acaba atacando os dispositivos para redes sem fio como, por exemplo, um *acess point* ou um cliente. [Air00]

As configurações inseguras, que costumam ser mantidas no caso anterior, podem ser comparadas a uma casa com portas de aço e paredes de vidro. Bruce Scheneier define a segurança como uma corrente, a qual é tão forte quanto seu elo mais fraco. Portanto, esta rede continua insegura.

Para minimizar o impacto das configurações inseguras, seria necessário modificar as configurações padrão de SSID, *broadcast* de SSID, criptografia fraca do WEP, por configurações mais robustas.

3.3.3 Associação Acidental

Muitos dos sistemas operacionais costumam configurar automaticamente os dispositivos para redes sem fio. Com o barateamento da tecnologia, a integração desta tecnologia em computadores pessoais, como *notebooks*, torna-se inevitável. Isso faz com que pessoas leigas desconheçam a existência deste dispositivo.

Outro fator importante é que mesmo sabendo da existência do dispositivo estas pessoas não sabem ao certo como configurar, manipular e gerenciá-lo. Assim sendo, existe uma grande possibilidade deste dispositivo se associar a outro dispositivo, sem o consentimento ou mesmo conhecimento do usuário. [Air00]

Um simples exemplo de como esta associação pode ocorrer esta relacionada a duas empresas A e B. Ambas possuem clientes e redes sem fio. Se o sinal da rede B invadir o campo de abrangência da rede A um cliente da rede A pode se associar acidentalmente à rede B. Além disso os *access points* de A podem se associar aos *access points* de B e criar uma ESS.

Uma forma de minimizar este tipo de risco que as redes sem fio estão expostos seria através da configuração manual do dispositivo. Ou ao menos não permitir que o dispositivo atue em modo *ad hoc*.

A importância em se prevenir a atuação em modo *ad hoc* ocorre, pois nestas redes não é preciso existir um *access point* para que os dispositivos se comuniquem. Com isso um atacante pode associar seu sistema ao sistema vítima sem a necessidade de se autenticar em um *access point* válido.

O sistema operacional Windows XP (*http://www.microsoft.com*), há bem pouco tempo, permitia a livre conexão dos dispositivos em modo *ad hoc* e/ou em redes sem criptografia. Hoje, já é necessária uma pequena intervenção do usuário.

3.4 Riscos Externos

Nos riscos externos, diferentemente dos internos, é exigida a interação direta dos atacantes para expor as vulnerabilidades. Muitos ataques inerentes a redes sem fio, são devidos aos riscos que serão apresentados.

3.4.1 *Eavesdropping & Espionage*

Este risco é muito parecido com o existente nas redes guiadas dos *sniffers* [NMR02]. O objetivo dos dois é o mesmo: Conseguir capturar e analisar todo o tráfego que passa pela rede. Utilizando os dados obtidos para gerar possíveis ataques ou roubar informações e senhas.

Entretanto, para que um atacante consiga obter o tráfego nas redes guiadas é necessário que este esteja dentro do mesmo domínio de colisão que a rede a qual deseja obter os pacotes. Ou seja, é necessário que o atacante tenha controle de pelo menos uma máquina ligada fisicamente à rede que pretende atacar.

No entanto, nas redes sem fio o sistema do atacante não precisa estar fisicamente ligado, nem associado a nem um dispositivo da rede alvo. Com isso, a identificação de quando um atacante efetua este tipo de ataque é muito mais complicada.

Eavesdropping & Espionage também introduzem uma vulnerabilidade ainda não comentada. Não existem, atualmente, mecanismos do próprio protocolo capazes de banir usuários não autenticados do tráfego da rede. Ou seja, uma forma eficaz de não permitir que estes ataques ocorram. Mesmo com a utilização de WEP as redes ainda permanecem vulneráveis.

Uma forma de tentar minimizar a ação deste tipo de ataque é através da utilização de VPNs, dificultando assim a escuta em detrimento da análise do tráfego pelo gerente da rede.

Um outro ponto importante que se relaciona a *Eavesdropping* é quanto a utilização de SDIs em redes sem fio. Como esta possui um concentrador de tráfego de saída (*access point*), é possível examinar o tráfego advindo destas redes depois do concentrador, extraindo o tráfego das VPNs e remontando-as após as análises.

3.4.2 Roubo de Identidade

O roubo de identidade ocorre quando um atacante consegue obter tantas informações quanto necessárias para poder se passar por um cliente válido da WLAN.

Muitas WLANs fazem a filtragem por endereços MAC. Com isso, mesmo que um atacante conheça o SSID da rede e saiba que a autenticação é aberta ele não consegue se associar à WLAN. O mesmo ocorre quando a WLAN não disponibiliza serviços de DHCP [Set94]. Então, para que o atacante possa usufruir a rede é necessário que ele obtenha um endereço MAC válido, bem como, um endereço IP também válido.

Através da utilização das técnicas anteriormente descritas o atacante pode obter, de um cliente válido, as informações de que precisa. Consegue então modificar seu endereço MAC e seu IP à semelhança da vítima. Conseguindo assim acesso a rede.

3.4.3 Ataques emergentes

Fazem parte destes ataques, aqueles que mais sofisticados como *Denial-of-Service* [NMR02] e *Man-in-the-Middle* [NMR02]. Estes ataques podem tornar as redes indisponíveis e comprometer a segurança de VPNs.

3.5 Ferramentas para redes sem fio

Antes de se analisar os ataques em redes sem fio, serão mostradas as ferramentas disponíveis tanto para a segurança quanto para o ataque nestas redes. A idéia é simplificar as explicações de cada um dos ataques e relacionar cada um destes com as ferramentas que utilizam.

As ferramentas também serão utilizadas para os experimentos práticos realizados. Como as ferramentas de ataque podem ser utilizadas para segurança e vice-versa, estas não serão classificadas quanto aos seus propósitos.

3.5.1 NetStumbler

URL: http://www.netstumbler.com

Este é a ferramenta mais conhecida de scanner para redes sem fio. Inclui muitas características como potência do sinal, ESSID da rede em questão, além de suporte a GPS. Este programa modificou significantemente o mundo da rede sem fio. Pois, além de ser utilizado para ações maliciosas, pode ser utilizado pelo gerente da rede em questão para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição.

Este software possui uma versão para *Pocket PC* intitulada *MiniStumbler*, a qual pode ser utilizada sem que desperte muita atenção e tenha a mesma eficácia do *NetStumbler* tradicional.

Apesar de todas as inovações trazidas por estes programas, a base de sua concepção também é a base de seu maior problema. Utilizando o método de sondagem ativa da rede, suas primeiras versões enviavam informações que facilitavam a identificação destes *softwares* através da análise do tráfego da rede.

3.5.2 Kismet

URL: http://www.kismetwireless.net

Desenvolvido com a filosofia *opensource*[13] este *sniffer* inclui um grande número de ferramentas e opções. Projetado como cliente e servidor, pode ter vários servidores rodando à distancia de um único cliente. Além de monitorar uma gama muito grande de origens diferentes, pode armazenar os pacotes capturados em vários formatos diferentes.

Além de funcionar como *sniffer*, este programa ainda gera dados relacionados à localização aproximada do dispositivo monitorado. Isto é realizado através da união das características do *Kismet* com um GPS. Outro ponto favorável em relação às outras ferramentas é que automaticamente salva todas as redes encontradas.

Trabalhando com a biblioteca *Ncurses*[14] e tendo várias telas e opções, disponibiliza quase todas as informações necessárias para um atacante desenvolver seus ataques. Algumas das informações que o *Kismet* consegue obter sobre o estado geral da sua área de abrangência são: Número de WLANs detectadas, número total de pacotes capturados por WLAN, ausência ou não de criptografia WEP, número de pacotes com o I.V. fraco, número de pacotes irreconhecíveis, número de pacotes descartados e tempo decorrido desde a execução do programa.

---

[13] Programas *opensource* – São programas que possuem seu código aberto, ou seja, qualquer pessoa com os conhecimentos necessários é capaz de alterar ou re-programar este código.

[14] *Ncurses* – É uma biblioteca para trabalho com ambientes com menus e telas, prove suporte a cor, negrito e outras funcionalidades, maiores informações podem ser obtidas em http://dickey.his.com/ncurses/ncurses.html.

Já outras informações a respeito de cada uma das WLANs encontradas são: SSID, BSSID (relaciona-se ao endereço MAC do *access point*), taxa máxima suportada pela rede, se o dispositivo monitorado é um *access point*, ou um dispositivo convencional, qual o canal que a WLAN esta configurada, se suporta WEP. Além disso, disponibiliza informações a respeito do intervalo de envio de *beacon frames*, mostra o total de pacotes capturados desta rede descrevendo quantos são de gerenciamento, quantos são de dados, quantos possuem criptografia e quantos são fracos.

O Kismet pode ainda disponibilizar quando o último pacote de determinada WLAN foi recebido, qual a qualidade do sinal deste ultimo pacote, qual a melhor qualidade de sinal já recebida e a pior.

Mais um ponto favorável ao *Kismet* é que este consegue relacionar os clientes das WLANs, bem como os IPs de cada um dos dispositivos. Estes endereços IPs podem ser descobertos através de requisições via ARP, via UDP e TCP. Além de trabalhar com sondagem passiva dificultando sobremaneira sua detecção.

Estas inúmeras características fazem com que o *Kismet* seja considerado, pelas análises nele realizadas, a ferramenta *opensource* para *Linux* mais completa e eficaz da atualidade.

3.5.3 Wellenreiter

URL: http://www.wellenreiter.net

Esta é uma ferramenta para descobrimento e auditoria de redes sem fio. Os testes realizados com esta ferramenta mostraram que esta não difere das demais. Entretanto, é mais rudimentar e insere poucas funcionalidades adicionais.

Uma destas funcionalidades é a capacidade de fazer um *brute force* dos SSIDs. Neste, a maioria dos SSIDs padrões são enviados em *broadcast* em pacotes de *Probe Request*[15] forjados com endereços MAC de origem adulterados. Assim, o *Wellenreiter* mantém o atacante oculto enquanto observa as respostas aos *Probes* que havia feito.

Hoje, o *Wellenreiter* esta disponível tanto em um script em *perl* e *gtk* como em C++. Tanto uma versão quanto outra foram testadas e nem uma das duas funcionou a contento, uma vez que a funcionalidade de *brute force* não pode ser efetuada, pois é necessária a existência de duas placas em um mesmo sistema.

3.5.4 Ethereal

URL http://www.ethereal.com

Este programa é de multipropósito, podendo ser utilizado tanto para segurança como para o ataque de redes. Inicialmente proposto para suportar os *Linktypes* das redes guiadas tem nas suas versões mais atuais suporte para redes sem fio.

---

[15] *Probe Request* - ou frames de requisição de informações discutido em 2.7)

Por depender da biblioteca de captura de pacotes *LibPcap,* no *linux*, este programa ainda possui algumas limitações no suporte das redes sem fio. Entretanto, estas limitações também afetam outros *softwares* como, por exemplo, o *Kismet*.

A utilização do *Ethereal* não se limita a sistemas *Linux*, podendo ser utilizando em outros sistemas comerciais. Entretanto os testes feitos com esta ferramenta mostraram que pacotes completos incluindo os cabeçalhos do *Prism II* e a porção de gerenciamento da rede sem fio possuem suporte somente para sistemas **nix*. Isso devido a falta de suporte na biblioteca *WinPcap*.

3.5.5 WEPCrack

URL: http://sourceforge.net/projects/wepcrack/

Este programa trabalha utilizando-se da vulnerabilidade encontrada no começo do ano 2001 no WEP. Na realidade este programa é um script *perl* e supostamente funcionaria em qualquer sistema com suporte a este tipo de script. No entanto, somente se torna inteiramente funcional em sistemas **nix*.

Pessoas mal intencionadas utilizam o *WEPCrack* para obter informações vitais à rede como o BSSID para gerar posteriores ataques.

3.5.6 AirSnort

URL: http://airsnort.shmoo.com

O *AirSnort* é um programa para quebra de chaves WEP. Funciona diferentemente do *WEPCrack*, pois consegue quebrar qualquer chave. Isto após conseguir obter aproximadamente de três a cinco milhões de pacotes trocados.

3.5.7 HostAP

URL:http://hostap.epitest.fi

Hostap é na realidade um módulo de *kernel* capaz de transformar um dispositivo de rede sem fio padrão em um *access point.* Máquinas convencionais podem, portanto, agirem como um *acess point*.

Este módulo além de ser utilizado em computadores pessoais, também podem ser instalados em *access points* através de uma modificação do *firmware* do mesmo.

Muitos atacantes utilizam-se das características providas por este módulo para gerar ataques de associação maliciosa e outros.

3.5.8 Orinoco/Wireless Tools

URL: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

O *Orinoco* também é um módulo que dá suporte a dispositivos de redes sem fio. Com o auxílio do conjunto de ferramentas *Wireless Tools*, torna possível a configuração de um cliente válido em uma rede.

Os comandos passíveis de serem executados diretamente nos dispositivos das placas de rede são retornados pelo comando *iwpriv*, como ilustrado na figura 3.1.

```
#iwpriv eth1
eth1      Available private ioctl :
          force_reset      (8BE0) : set   0       & get   0
          card_reset       (8BE1) : set   0       & get   0
          set_port3        (8BE2) : set   1 int   & get   0
          get_port3        (8BE3) : set   0       & get   1 int
          set_preamble     (8BE4) : set   1 int   & get   0
          get_preamble     (8BE5) : set   0       & get   1 int
          set_ibssport     (8BE6) : set   1 int   & get   0
          get_ibssport     (8BE7) : set   0       & get   1 int
```

Figura 3.1 – Saída do comando *iwpriv* – ambiente de análise

Outro comando que disponibiliza e seta as configurações da WLAN é o *iwconfig*, figura 3.2 .

```
#iwconfig eth1
eth1      IEEE 802.11-DS  ESSID:"linksys"  Nickname:"Prism  I"
          Mode:Managed  Frequency:2.437GHz  Access Point: 00:06:25:A2:XX:XX
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity:1/3
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0/92  Signal level:-68 dBm  Noise level:-122 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 3.2 – Saída do comando *iwconfig* – ambiente de análise

Observa-se, por exemplo, qual o ESSID, o *chipset*, o modo em que a placa está operando, freqüência e conseqüente canal, sensibilidade entre outros.

O *Wireless Tools* é indispensável para ambientes *Linux*, mesmo que os dispositivos necessitem de outros módulos que não o *Orinoco*. Visto que atualmente é o único capaz de modificar determinadas opções das redes sem fio.

3.6 Ataques às redes sem fio

Os ataques às redes sem fio não são novos. Ao invés disso, eles são baseados em ataques anteriormente descobertos em redes guiadas. Alguns destes ataques não sofreram nem uma modificação, já outros sofrem algumas modificações para que possam ser disparados e obter melhores resultados.

Na realidade, o objetivo dos ataques não é comprometer a rede sem fio, mas sim ganhar acesso ou comprometer a rede guiada.

Como as redes guiadas tradicionais tem sido duramente atacadas durante mais de trinta anos, muitas desenvolveram excelentes defesas. Por exemplo, o uso de um *firewall* propriamente configurado pode aumentar sensivelmente o nível de segurança da instituição. Entretanto, se esta mesma instituição possuir uma rede sem fio mal configurada atrás deste *firewall*, é como se existisse um *backdoor* [NMR02] devidamente instalado.

Atualmente, a maioria das WLANs irão certamente sofrer de pelo menos um tipo de ataque[PF02]. Estes ataques não são limitados a instituições, visto que o maior número de equipamentos deste tipo de rede é vendido para consumidores domésticos. Os quais procuram aumentar sua largura de banda ou distribuir sua conexão em toda sua residência.

Serão apresentados a seguir os ataques que mais se destacam atualmente nas redes sem fio.

3.6.1 Associação Maliciosa

A associação maliciosa ocorre quando um atacante passando-se por um *access point*, ilude outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real. [Air00]

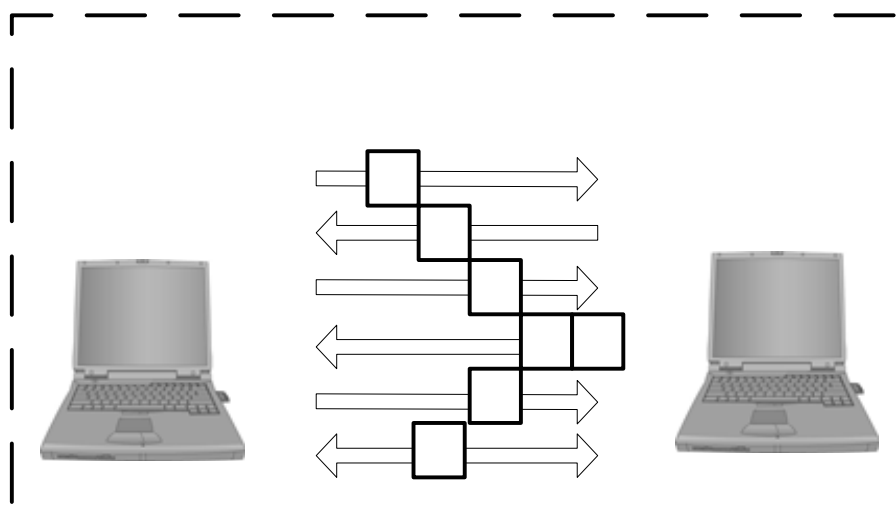



Figura 3.3 – Associação Maliciosa.

Esta associação maliciosa, comprovada em nosso ambiente experimental, consta de duas máquinas com dispositivos para redes sem fio e segue o seguinte conjunto de passos:

1. A vítima envia pacotes de *Probe Request* à procura de *access points* para conexão;
2. O atacante com o auxílio de um *softAP*[16] responde a conexão;
3. A vítima requisita a associação e se associa ao atacante;
4. O atacante responde com as informações de rede necessárias como endereço IP;
5. O atacante envia uma requisição de NET USE;
6. A vítima responde com LOGIN;
7. Qualquer vulnerabilidade de qualquer serviço do cliente pode ser agora explorada.

Neste exemplo, o atacante tenta se valer de uma vulnerabilidade do *NETBEUI* que permite compartilhamento de arquivos e impressoras em sistemas *Windows*. Entretanto a partir do passo quatro, qualquer vulnerabilidade existente no cliente pode ser explorada pelo atacante.

Existe uma sutil diferença entre fazer a associação maliciosa através da utilização de um *softAP* ou da associação através de redes *Ad Hoc*. Esta diferença está na grande difusão dos riscos em se manter um dispositivo configurado para atuar em *Ad Hoc*. Com isso muitos usuários e até mesmo sistemas operacionais evitam este tipo de conexão. Permitindo somente conexões em sistemas de infra-estrutura básica ou sistemas infra-estruturados.

3.6.2 ARP Poisoning

O ataque de envenenamento do protocolo de resolução de endereços (ARP) é um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vitima. Limitando este ataque às redes que estejam conectadas por *hubs, switches* e *bridges*. Deixando de fora as redes conectadas por roteadores e *gateways*.

Muitos dos *access points* disponíveis hoje no mercado atuam com um *bridge* ente a rede guiada e a rede sem fio. Desta forma, um ataque que se utilize de *ARP Poisoning* como é o caso do ataque do Homen-no-Meio pode ser disparado de uma estação da WLAN à uma estação guiada. Ou seja, este ataque não fica restrito apenas às estações sem fio.

O ataque de *ARP Poisoning* não é um ataque novo, porém a forma de concepção dos *access points* e a implicação da arquitetura de rede gerada por este *access point* faz com que esta rede seja particularmente vulnerável a esta forma de ataque.

A maneira como o ataque é convencionalmente disparado em redes guiadas é demonstrado a seguir. Para maiores informações sobre o funcionamento do ARP consulte [Ste94].

[16] *softAP* são programas capazes de transformar um dispositivo de rede padrão em um *access point*. Um exemplo de programa muito utilizado é o *HostAP* discutido no item 3.5

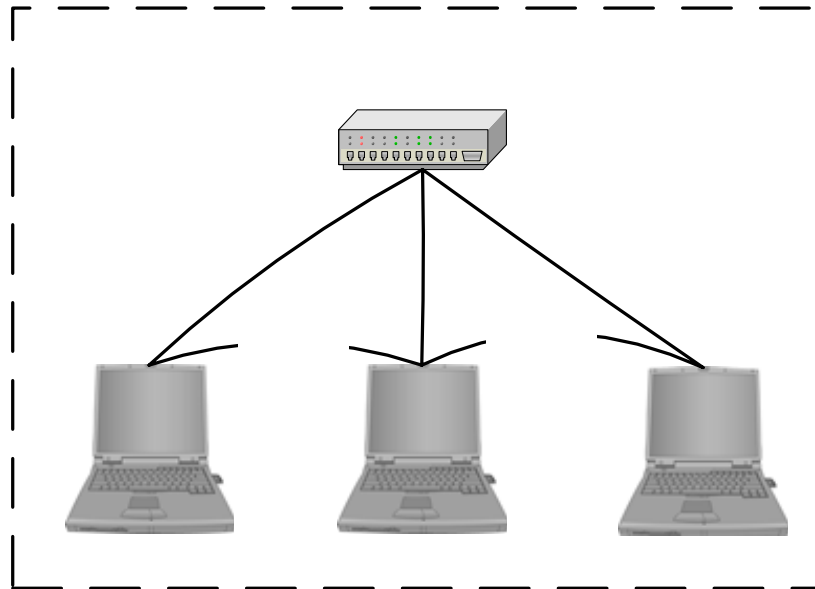



Figura 3.4 – ARP Poisoning em redes guiadas

Este ataque utiliza-se de pacotes de *ARP reply* para fazer o *cache poisoning*. O atacante, host C, envia um pacote de *ARP reply* para B dizendo que o IP de A aponta para o endereço MAC de C. De maneira semelhante envia um pacote de *ARP reply* para A dizendo que o IP de B aponta para o endereço MAC de C. Como o protocolo ARP não guarda os estados, os hosts A e B assumem que enviaram um pacote de ARP request pedindo estas informações e assumirem os pacotes como verdadeiros.

A partir deste ponto, todos os pacotes trocados entre os *hosts* A e B necessariamente passam por C. Portanto o *host* C deve se encarregar de reenviar os pacotes para os devidos destinos após capturá-los.

Nas redes sem fio este ataque pode ser disparado e desenvolvido de várias formas diferentes. Estas formas podem ser verificadas no anexo B.

3.6.3 MAC Spoofing

Existem muitas instituições que criam listas de acesso para todos os dispositivos explicitamente permitidos à conexão. Estas instituições costumam fazer este controle através do endereço MAC da placa do cliente. Banindo desta forma o acesso de outras placas não autorizadas.

Entretanto, os dispositivos para redes sem fio possuem a particularidade de permitir a troca do endereço físico. Com isso, atacantes mal intencionados podem capturar através de técnicas de *Eavesdrooping & Espionage* um endereço MAC válido de um cliente, trocar seu endereço pelo do cliente e utilizar a rede.

Além deste tipo de *MAC Spoffing*, existe o *MAC Spoffing* da placa de rede guiada dos *access points*. Ou seja, os *access points* são capazes de trocar seus endereços MAC das placas de redes tradicionais burlando assim os *firewall* internos á LAN.

Para comprovar esta facilidade, seguem os resultados de comandos entrados para a modificação do MAC, executados no ambiente de análises.

```
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:02:2D:3D:4F:3C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1623 (1.5 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100

#ifconfig eth0 down
#ifconfig eth0 hw ether 1B:11:CE:DC:CE:00
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 1B:11:CE:DC:CE:00
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1659 (1.6 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100
```

Figura 3.5 – MAC Spoffing – Sanitizado

3.6.4 D.o.S

Ataques de *Denail of Service* (D.o.S – Negativa de Serviço) como o nome próprio indica, procura tornar algum recurso ou serviço indisponível. Em redes sem fio estes ataques podem ser tão perturbadores quanto maior sua sofisticação.

Estes ataques podem ser disparados de qualquer lugar dentro da área de cobertura da WLAN. Como as redes 802.11b/g trabalham na radiofreqüência de 2.4 GHz e esta é utilizada por fornos microondas, aparelhos de monitoramento de crianças e recentemente por telefones sem fio, estes produtos podem facilitar os ataques de negativa de serviço. Através da inserção de ruídos a partir destes aparelhos nas redes sem fio.

Entretanto, *hackers* podem gerar ataques mais sofisticados. Por exemplo, um atacante pode se passar por um *access point* com o mesmo SSID e endereço MAC de um outro *acess point* válido e inundar a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se re-associarem. Enviando as requisições de dissociação em períodos curtos de tempo o D.o.S é concretizado. Isso, pois os clientes não conseguiriam permanecer conectados por muito tempo.

3.6.5 Ataques de Vigilância

Ataque de vigilância, apesar de não ser considerado ataque para muitos estudiosos, pode se tornar um ataque com um grau de comprometimento muito grande dependendo da finalidade para a qual este ataque é efetuado.

Este ataque consiste em se percorrer a cidade ou a instituição, a qual se deseja "vigiar", apenas observando a existência ou não de WLANs. Para tanto, não existe a necessidade de nem um equipamento especial.

A idéia por trás deste ataque é encontrar fisicamente os dispositivos de redes sem fio para que estes dispositivos possam, posteriormente, ser invadidos. Podendo ainda ter sua configuração *resetada* à configuração padrão ou ainda ser roubado.

No caso em que um *access point* pode ser *resetado*, um atacante pode invadí-lo, conseguindo gerar ataques dentro da porção guiada da rede. Representando assim um grande risco a exposição de equipamentos.

3.6.6 Wardriving

Wardriving é uma forma de ataque muito parecida com a anterior. Modifica-se somente a forma de como as WLANs são encontradas. Utilizam-se neste tipo de ataque equipamentos configurados para encontrar tantas redes sem fio quantas aquelas que estiverem dentro da área de abrangência do dispositivo de monitoramento.

O objetivo deste tipo de ataque, além dos já mencionados nos ataques de vigilância é mapear todos os *access points* encontrados com o auxilio de um GPS (*Global Position System*).

Muitas *homepages* como o "wardriving.com"[17] dão instruções detalhadas de como efetuar o *wardriving*. Outras como a "wardriving is not a crime"[18] tem como tem como principal objetivo fazer apologia ao *wardriving*.

O que mais chama atenção é a distribuição *WarLinux*[19] concebida única e exclusivamente para *wardriving*.

3.6.7 Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de *wardriving* e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. Isto para que outros atacantes possam de antemão saber quais as características da rede.

Alguns dos símbolos utilizados por estes atacantes podem ser observados na figura a seguir. Existem grupos organizados para *warchalking* que se utilizam de símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo.

Existem também grupos rivais que tentam encontrar e pichar o maior número de redes possível para ganhar mais status. Seriam como os grupos de *defacers* de páginas da *Web*, mas realizados fisicamente.

[17] Wardriving.com - http://www.wardriving.com/
[18] Wardriving is not a crime - http://www.wardrivingisnotacrime.com
[19] WarLinux - https://sourceforge.net/project/showfiles.php?group_id=57253

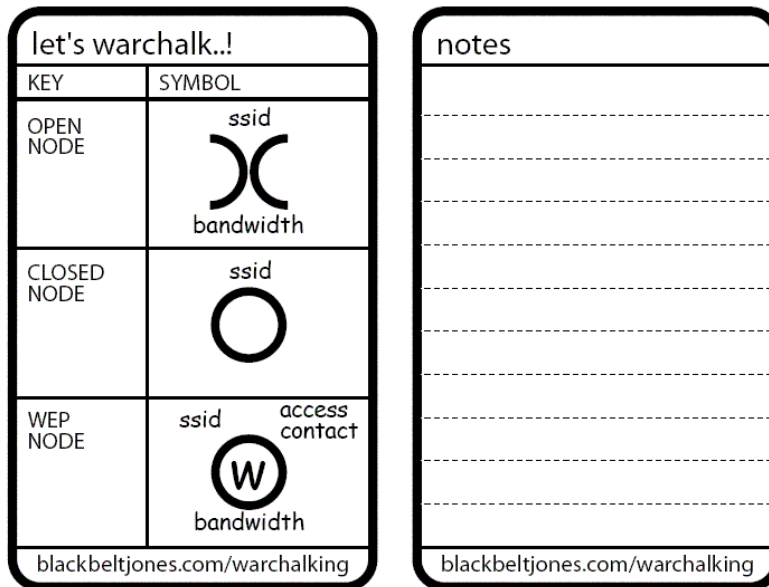



Figura 3.6 – Símbolos de *Warchalking*

3.7 Ambiente dos testes experimentais

O objetivo dos testes realizados é essencialmente comprovar a existência de uma dada vulnerabilidade, bem como validar as técnicas de ataques encontradas. Apesar destes testes não terem sido efetuados para todos os ataques apresentados neste trabalho, pode-se garantir com total certeza a eficácia de todos.

3.7.1 Equipamentos

Tabela 3.1 – Ambiente de análise

Dispositivo	Sistema Operacional	Placa de rede *wireless*
Desktop Pentium III / 800MHz / 512MB	Red Hat 9 com kernel 2.4.20 (vanilla)	3com PCI - 3CRDW696
Desktop Pentium III / 800MHz / 512MB	Red Hat 8 com kernel 2.4.18 (vanilla) / Windows XP	Linksys PCI - WMP11
Notebook Pentium III / 800MHz / 128MB	Gentoo com kernel 2.4.20 / 2.4.18 (vanilla)	Dell TrueMobile PCMCIA – 1150 series / 3com PCMCIA - 3CRWE62092A
Desktop Pentium – 100 MHz/32MB	Freebsd 5.0	3com PCI - 3CRDW696
Access point LINKSYS	-	Built-in – Linksys
Access point LINKSYS	-	Built-in – Linksys
Access point LINKSYS	-	Built-in – Linksys

Estes equipamentos foram dispostos de várias formas diferentes para garantir que cada um dos experimentos fosse executado da melhor maneira possível.

3.7.2 Comprovando *Eavesdropping & Espionage*

Para comprovar a possibilidade da captura dos pacotes nas redes sem fio, houve a necessidade da instalação, no *desktop* Pentium III com *red hat* 9, de um módulo de *kernel* capaz de permitir a captura completa dos pacotes das redes sem fio.

Entretanto, o módulo *orinoco* original não envia informações sobre os *frames* de gerenciamento das redes sem fio, necessitando da aplicação de um *patch* para realizar a captura dos mesmos. A figura a seguir mostra a saída do comando *iwconfig*, contendo as características das configurações do dispositivo, como o canal (freqüência), a presença ou não de criptografia e o SSID. Não há diferenças significativas em relação ao módulo sem *patch*.

```
#iwconfig eth1
eth1     IEEE 802.11-DS  ESSID:"non-specified SSID"  Nickname:"HERMES I"
          Mode:Managed       Frequency:2.437GHz       Access       Point:
00:00:00:00:00:00
          Bit Rate:2Mb/s Tx-Power=15 dBm   Sensitivity:1/3
          Retry limit:4   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0/92  Signal level:134/153  Noise level:134/153
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 3.7 – Saída do comando *iwconfig*.

Entretanto, diferenças podem ser vistas com o comando *iwpriv*, como a operação em modo *monitor*. Este modo permite a captura de todos os pacotes dentro da área de cobertura do dispositivo, fazendo com que o mesmo opere de maneira passiva (sem trocar dados com as demais estações).

Há duas opções de funcionamento: uma permite a captura com o cabeçalho do *PRISM II*, recomendada para análise integral do tráfego. Já a outra suprime o cabeçalho.

```
#iwpriv eth1
eth1      Available private ioctl :
          force_reset      (8BE0) : set   0       & get   0
          card_reset       (8BE1) : set   0       & get   0
          set_port3        (8BE2) : set   1 int   & get   0
          get_port3        (8BE3) : set   0       & get   1 int
          set_preamble     (8BE4) : set   1 int   & get   0
          get_preamble     (8BE5) : set   0       & get   1 int
          set_ibssport     (8BE6) : set   1 int   & get   0
          get_ibssport     (8BE7) : set   0       & get   1 int
          monitor          (8BE8) : set   2 int   & get   0
          dump_recs        (8BFF) : set   0       & get   0
```

Figura 3.8 – Saída do comando *iwpriv*.

Unindo-se a este módulo, a *libpcap*[20] – *v.0.7.2* e *cvs.2003.06.02*, foram utilizadas pois suportam pacotes provenientes de interfaces de redes sem fio. Esta captura é possível devido a algumas alterações que inseridas da biblioteca, as quais serão observadas a seguir.

[20] LibPcap - *http://www.tcpdump.org*

Utilizou-se ainda, os *softwares Ethereal* e *Kismet* para a captura e sondagem de uma WLAN montada com um *access point* e um cliente. Validando assim a capacidade de total captura de pacotes nas redes sem fio.

3.7.2.1 Modificações na *libpcap*

As alterações feitas na *libpcap* têm por objetivo permitir a interpretação dos pacotes oriundos de redes sem fio, sendo introduzidas diretamente no código. As principais foram o suporte para o *link type* 119 (cabeçalho do *PRISM II*) e *link type* 105 (802.11).

Por tais suportes serem recentes na *libpcap*, ainda existem limitações que precisam ser superadas, como o tamanho do cabeçalho 802.11, que é variável enquanto que na biblioteca um valor fixo padrão de 24 *bytes* é assumido.

Ainda assim a biblioteca é bastante robusta e consegue tratar a grande maioria dos pacotes de redes 802.11.

3.7.3 Validando Associação maliciosa.

Para este experimento foram utilizados o *desktop* Pentium III com *redhat* 9 e o *notebook* com *Geento*. Sendo que o *desktop* foi configurado com o módulo *Hostap* (que permite que o dispositivo trabalhe a semelhança de um *access point*) e o *notebook* com o sistema operacional *Windows XP* sem nem uma atualização.

Comprova-se que neste caso o cliente *Windows XP* conecta-se ao *access point* forjado, comprovando desta forma que o ataque de associação maliciosa é perfeitamente factível.

3.7.4 Validando ARP *poisoning*

Para validar o ataque do tipo ARP *poisoning*, foram utilizados os dois *desktops* Pentium III como vítimas. Um rodando *Windows XP* e outro rodando *red hat* 9. Para o atacante foi configurado o *notebook* com *Gentoo*. Além de um *access point*.

O objetivo é comprovar o ataque onde todos os clientes estejam conectados no mesmo *access point* é viável. Para tanto, foi utilizado o software *Ettercap*[21], o qual implementa ARP *poisoning* por *cache poisoning*, para efetuar o ataque.

De maneira satisfatória o ataque foi efetuado e comprovado em sua forma mais simples, onde todos os usuários estão conectados ao mesmo *access point*.

[21] Ettercap: htttp://ettercap.sourceforge.net/

3.7.5 Validando MAC *spoofing*

Este teste foi realizado no *notebook* com *Geento* e os resultados podem ser observados na figura 3.5. Não existe a necessidade de nem um comando especial que não os apresentados na figura. Comprovando assim a eficácia deste ataque.

3.8 Considerações Finais

Neste capítulo, foram analisadas as vulnerabilidades inerentes às redes sem fio. Mostrando como estas vulnerabilidades podem ser exploradas e como um eventual atacante pode se valer destas para comprometer o sistema alvo.

Foi mostrado também o ambientes experimental montado para a validação de algumas das vulnerabilidades através de ferramentas desenvolvidas para invasão de redes sem fio. Ferramentas estas que estão disponíveis na Internet e são de domínio público.

Como visto neste capítulo, as vulnerabilidades presentes nas redes sem fio podem causar prejuízos tanto financeiros como lógicos às instituições. Por isso, medidas para minimizar as vulnerabilidades, devem ser desenvolvidas e seguidas para que as perdas com eventuais ataques sejam diminutas.

4

"Please put down your weapon. You have 20 seconds to comply..."
ED 209 – *RoboCop*

Conclusão

Este projeto envolveu o estudo de protocolos, comportamentos ofensivos em redes sem fio e estudo das ferramentas de uso malicioso. A necessidade de estudos em diversas áreas diferentes do conhecimento possibilitou um grande aprendizado nestas áreas.

A insegurança ilustrada nos capítulos anteriores de fato afetam cotidianamente as redes sem fio de computadores, visto o resultado de outros estudos desenvolvidos no laboratório no sentido de quantificar e qualificar estas redes. Entretanto, muitos grupos estudam formas de banir as vulnerabilidades e não permitir que os ataques ocorram.

Apesar do extremismo em afirmar as vulnerabilidades existentes nas redes sem fio, algumas destas não podem ser trivialmente exploradas. Ou seja, somente um atacante com um bom grau de conhecimento da tecnologia é capaz de dispará-los, o que de certa forma mantém estas vulnerabilidades ocultas.

As ferramentas citadas anteriormente são em sua grande maioria encontradas com facilidade na rede mundial de computadores o que também aumenta a insegurança das redes. Além de existir, hoje, suporte para a conexão em computadores como *handhelds*, o que faz com que atacantes possam passar desapercebidos e ter maior mobilidade.

Apesar de ter o propósito de analisar e estudar os ataques das redes sem fio, por ter um tamanho limitado, este trabalho trata apenas daqueles mais conhecidos. Além disso, mesmo que fossem cobertos todos os ataques conhecidos, isto não seria um indicativo de que outros ataques e outras vulnerabilidade não pudessem ocorrer.

Quanto às análises um ponto importante que deve ser ressaltado é que neste projeto somente foram feitas as análises dos módulos efetivamente firmados pelo IEEE e que dão suporte a redes sem fio. Outros padrões como o WPA desenvolvido pela *WiFi Alliance* não formam estudados.

4.1 Propostas para trabalhos futuros

Serão apresentados os trabalhos que poderiam ser desenvolvidos a partir deste. Podendo, portanto, dar continuidade à esta pesquisa.

O estudo de alternativas para banir as vulnerabilidades e os ataques conhecidos das redes sem fio é uma proposta de trabalho que vem de encontro a este. Visto que esta seria uma pesquisa complementar a já executada.

Através da pesquisa realizada neste projeto, é possível encontrar muitas medidas de segurança perfeitamente cabíveis e de fácil aplicação em redes domésticas convencionais. Juntamente com estas medidas foram encontradas outras mais técnicas que precisam de um grau de conhecimento maior dos sistemas. Por isso o estudo e a junção de várias medidas para que se seja possível gerar um padrão de segurança em redes sem fio é extremamente necessário.

Outra proposta seria ligada à obtenção de alguma ferramenta automatizada capaz de identificar quando uma rede esta sendo atacada através da exploração de alguma destas vulnerabilidades apresentadas. Sendo assim um trabalho mais voltado a prática da segurança.

Esta proposta tem como idéia principal a montagem de um identificador de intrusão capaz para redes sem fio. Onde as assinaturas de ataques são em sua grande parte geradas na camada II do modelo OSI.

Uma outra proposta seria o estudo de formas para identificação precisa das origens dos ataques. Em redes guiadas, fazer o *backtracking* de ataques é muito complicado, entretanto em redes sem fio o atacante normalmente esta a poucos metros da instituição atacada. Com isso, efetivamente localizar o atacante é teoricamente mais fácil. Alguns estudos levam em consideração a abordagem de triangulação por potencia de sinais para realizar a localização geográfica do atacante.

REFERÊNCIAS BIBLIOGRÁFICAS

[Air00] AirDefense White Paper, "*Wireless LAN Security – What Hackers Know That You Don't*", http://www.airdefense.net (verificado em 02 de abril de 2003).

[ASW01] Arbaugh, W.A.; Shankar, N. e Wan, Y.C.J., "*Your 802.11 Wireless Network has No Clothes*", University of Maryland Departament of Computer Science, 2001.

[BV98] Blunk, L. e Vollbrecht, J., "*PPP Extensible Authentication Protocol (EAP)*", Tech. Rep. RFC2284, Internet Engineering Task Force (IETF), 1998.

[FBA98] Forouzan, B. A., "*Introduction to data communications and networking*", McGRAW-HILL International Editions, 1998.

[FD02] Fleck, B. e Dimov, J., "*Wireless Access Points and ARP Poisoning*", Cigital, Inc., 2002

[FER98] Ferguson, P. "*What is a VPN?*", 1998, http://www.employees.org/~freguson/vpn.pdf, (verificado em 16 de setembro de 2003).

[IEE03a] IEEE Standard, 802.11g, "*(Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)*", 2003

[IEE03b] IEEE Standard for IT-Telecommunications and information exchange between systems LAN/MAN, "*Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*", 2003

[IEE97] LAN MAN Standards of the IEEE Computer Society, "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification, IEEE Standard 802.11, 1997 Edition*", 1997.

[IEE99] LAN MAN Standards of the IEEE Computer Society, "*Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*", 1999.

[IEE99a] ANSI/IEEE Standard, 802.11a, "*Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band*", 1999.

[IEE99b] ANSI/IEEE Standard, 802.11b, "*Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band*", 1999.

[IET03] IETF - *Internet Engineering Task Force*, http://www.ietf.org (verificado em 16 de setembro de 2003).

[ISO03] ISOC – *Internet Society*, http://www.isoc.org (verificado em 16 de setembro de 2003).

[ISO89] International Organization for Standardization, "*Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*", Intenational Standard 7498-2, 1989

[KR01] Kurose, J. F. e Ross, K. W., "*Computer Networking: A Top-Down Approach Featuring the Internet*", Addison Wesley, 2001.

[KR02] Regan, K., "*Wireless LAN Security: Things You Should Know about WLAN Security*", Cisco System, 2002.

[MA02] Mishra, A., Arbaugh, W. A., *"An Initial Security of the IEEE 802.1x Standard"*, Departamet of Computer Science University of Maryland, 2002.

[NMR02] Murillo, N. M. de O., "Segurança Nacional", Novatec Editora Ltda., 2002.

[PF02] Peikari, C. e Fogie S., *"Wireless Maximum Security"*, Sams, 2002

[RFC-791] RFC 791: Internet Protocol, http://www.ietf.org/rfc/rfc791.txt (verificado em 16 de setembro de 2003).

[RFC-793] RFC 793: Transmission Control Protocol, http://www.ietf.org/rfc/rfc793.txt (verificado em 16 de setembro de 2003).

[Sou02] Souza, M., "Readaptação do Modelo ACME! para detecção de novas técnicas de intrusão.", Projeto final de graduação apresentada ao Departamento de Ciência da Computação e Estatística de São José do Rio Preto, Universidade do estado de São Paulo, 2002.

[SSK01] Singhal, S. K., "*Understanding Wireless LAN Security*", ReefEdge, 2001

[Ste94] Stevens, W. R., "*TCP/IP Illustrated – The Protocols*", Addison Wesley, 1994.

[VM02] Volbrecht, J. e Moskovitz, R.; "*Wireless LAN Access control and Authentication*", http://www.interlinknetworks.com (verificado em 02 de abril de 2003), 2002.

[WH02] Arcomano, R., "*Wireless Howto*", http://tldp.org (verificado em 02 de abril de 2003), 2002.

[WiF03] Wi-Fi Alliance, http://www.weca.net/OpenSection/index.asp (verificado em 16 de setembro de 2003).

[WJ02] Wright, J., "*Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection*", http://home.jwu.edu/jwright/ (verificado em 02 de abril de 2003), 2002.

[WPA02] Grimm, C. B., "*Wi-Fi Protected Access*", http://www.weca.net/OpenSection/pdf/wi-fi_protected_access_overview.pdf (verificado em 16 de setembro de 2003), 2002.

[ZCC00] Zwicky, E. D., Cooper, S., Chapman, D. B. "*Building Internet Firewalls*", Segunda edição, O'Reilly, 2000.

ANEXO A

Beacon Frame

Neste anexo se encontram informações adicionais referentes aos pacotes de *beacon frames* enviados pelos *access points*. O pacote ilustrado a seguir foi capturado no ambiente experimental citado no capítulo 3. Utilizando-se o *notebook Fujitsu FMV-Biblo NE5/800HR* com a placa *Dell TrueMobile*. Além da utilização de um *access point* da marca *Linksys*.

Três protocolos podem ser identificados no pacote da figura A.1. O primeiro deles é o *Prism Monitor Header* que é o cabeçalho do *Prism II*, o qual não é inserido no pacote pela origem, e sim pelo destino. O seu intuito é permitir que informações importantes, como sinal *(Signal)*, ruído *(Noise)* e taxa de transmissão *(Rate),* possam ser obtidas. O campo *Signal* informa com qual potência de sinal o pacote chega ao dispositivo de monitoramento, permitido identificar se o emissor está ou não próximo ao receptor. O campo *Noise* identifica as interferências presentes na radiofreqüência no momento da transmissão do pacote, enquanto *Rate* ilustra qual a taxa de transmissão do pacote.

O segundo protocolo é o *IEEE 802.11* e, como o primeiro, está presente em todos os pacotes trocados entre os dispositivos de redes sem fio. Informações relevantes, como a presença ou não de criptografia WEP *(WEP flag)*, fragmentação *(More Fragments)*, retransmissão *(Retry)*, presença de dados bufferizados *(More Data)*, número de seqüência do pacote *(Sequence Number)* e os endereços, podem ser identificadas. No pacote de exemplo observa-se que o valor do campo *Type/Subtype* representa um *beacon frame* o qual é enviado em *broadcast* pelo *access point.*

O terceiro protocolo encontrado neste pacote é o *IEEE 802.11 wireless LAN management frame* que é o *frame* de gerenciamento do IEEE 802.11. Ocorre somente em pacotes sem dados de aplicação e tem como objetivo o controle da WLAN. Em um *beacon frame*, informações como SSID (*SSID*), taxas suportadas (*supported rates*) e canal de atuação (*current channel*) do *access point* são identificadas.

Observa-se que este pacote possui no seu *Tag interpretation* referente ao *Tag Number: 0* a string “linksys” que identifica o SSID da WLAN em questão.

```
# tethereal -r beacon_frame.dump -V
Prism Monitoring Header
    Message Code: 65
    Message Length: 144
    Device: eth1
    Host Time: 0x4da148 (DID 0x1041, Status 0x0, Length 0x4)
    MAC Time: 0x8d826845 (DID 0x2041, Status 0x0, Length 0x4)
    Channel Time: 0x0 (DID 0x3041, Status 0x1, Length 0x4)
    RSSI: 0x0 (DID 0x4041, Status 0x1, Length 0x4)
    SQ: 0x0 (DID 0x5041, Status 0x1, Length 0x4)
    Signal: 0x2d (DID 0x6041, Status 0x0, Length 0x4)
    Noise: 0x0 (DID 0x7041, Status 0x0, Length 0x4)
    Rate: 0x4 (DID 0x8041, Status 0x0, Length 0x4)
    IsTX: 0x0 (DID 0x9041, Status 0x0, Length 0x4)
    Frame Length: 0x3c (DID 0xa041, Status 0x0, Length 0x4)
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From
DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:06:25:a2:XX:XX (00:06:25:a2:XX:XX)
    BSS Id: 00:06:25:a2:XX:XX (00:06:25:a2:XX:XX)
    Fragment number: 0
    Sequence number: 1826
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000578337720E
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0001
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator at AP
(0x0000)
            .... .... ...0 .... = Privacy: AP/STA cannot support WEP
            .... .... ..0. .... = Short Preamble: Short preamble not allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .0.. .... .... = Short Slot Time: Short slot time not in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
    Tagged parameters (24 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 7
        Tag interpretation: linksys
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbits/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 0, DTIM period 3, Bitmap control 0x0, (Bitmap
suppressed)
```

Figura A.1 – *Beacon frame* capturado – dados sanitizados

ANEXO B

ARP *poisoning* em redes sem fio

Neste anexo se encontram maiores informações sobre ataques tipo Arp *poisoning* em redes sem fio que foram citados na secção 3.6.2.

➲ **Ataque sem fio como na rede guiada**

Neste ataque ao invés de termos três sistemas envolvidos e ligados diretamente na rede guiada, temos três dispositivos interligados na rede sem fio. O ataque pode ser observado na figura a seguir.

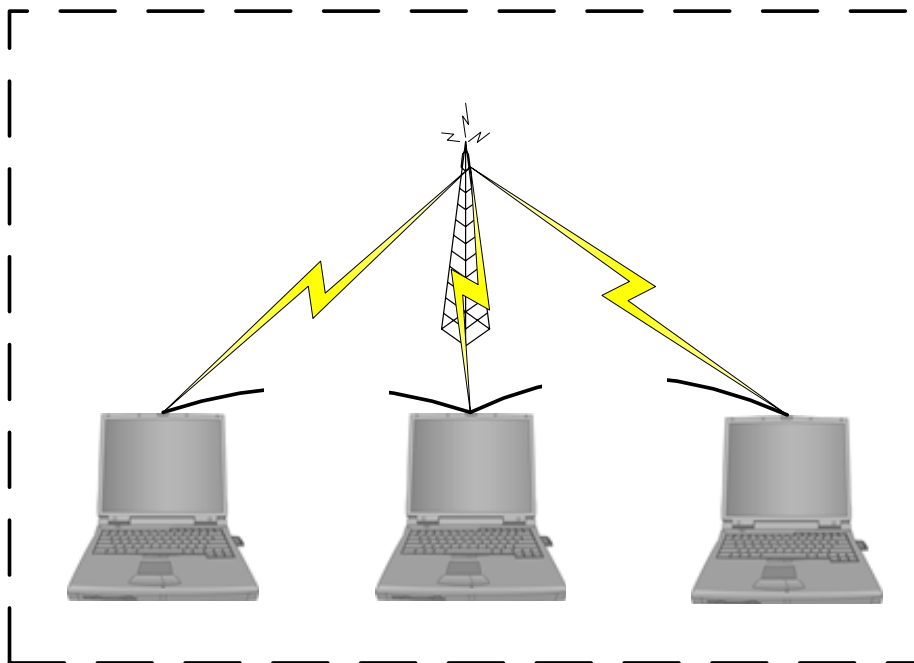



Figura B.1 – Wireless ARP Poisoning: 3 *hosts* na porção sem fio.

➲ **Ataque a vítimas cabeadas de uma posição sem fio**

O ataque, como ilustrado na figura abaixo, apesar de semelhante aos ataques anteriores insere um novo risco às redes. Ou seja, a possibilidade de um atacante externo a rede conseguir obter dados válidos de clientes guiados. Este ataque é possível, pois o atacante e as vítimas estão no mesmo domínio de *broadcast*. Esta peculiaridade aumenta ainda mais o nível de insegurança da rede.

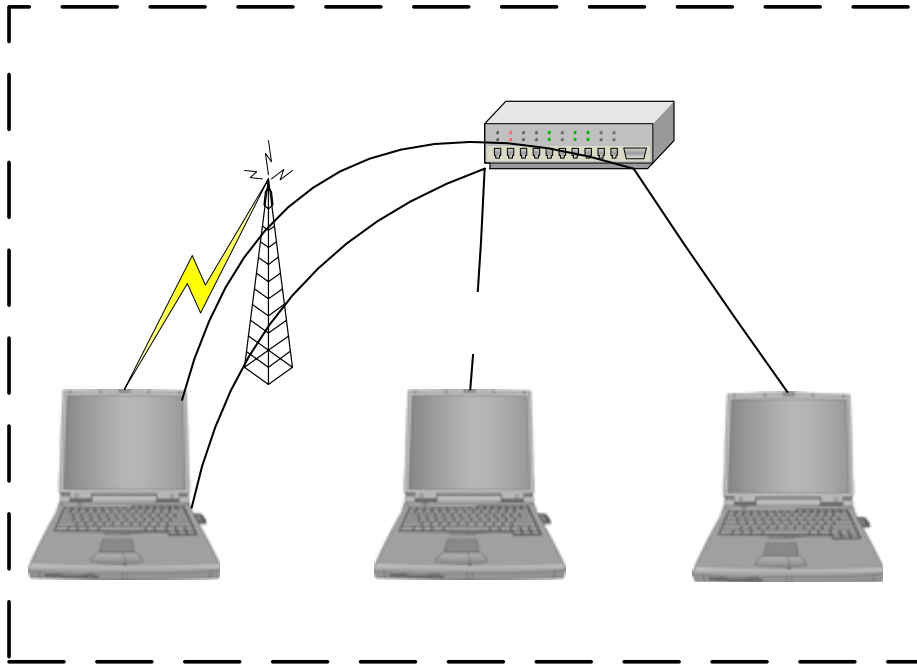



Figura B.2 – Wireless ARP Poisoning: 2 *hosts* na porção guiada e 1 na sem fio.

➲ **Ataque a uma vítima guiada e uma sem fio**

Um atacante pode gerar uma ataque de Homen-no-Meio contra um cliente que esteja na porção sem fio da rede, conectado à um sistema da rede guiada. Como os dois sistemas alvo estão no mesmo domínio de *broadcast*, o ataque através de *cache poisoning* é possível, como ilustrado a seguir.

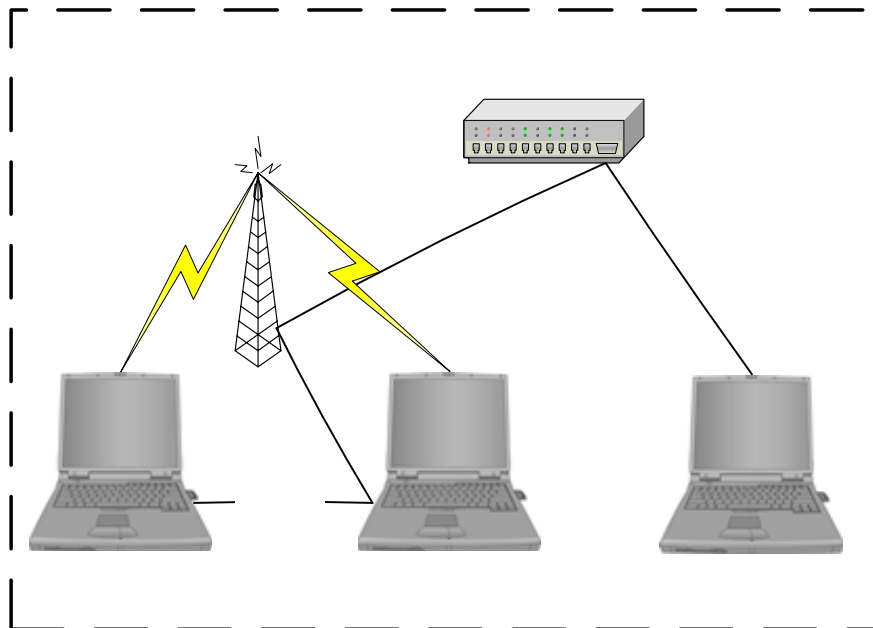



Figura B.3 – Wireless ARP Poisoning: 1 host na porção guiada e 2 na sem fio.

➲ Ataque a vítimas sem fio em *roaming*

Como ilustrado na figura a seguir, existe a possibilidade de que ataques de *ARP Poisoning* sejam disparados contra dois *hosts* em *access points* diferentes. Entretanto, deve-se observar que estes devem estar ligados em um *switch* ou um *hub*. Isto tanto para o conceito de *roaming* ser válido quanto para que os dispositivos estejam dentro de mesmo domínio de *broadcast*.

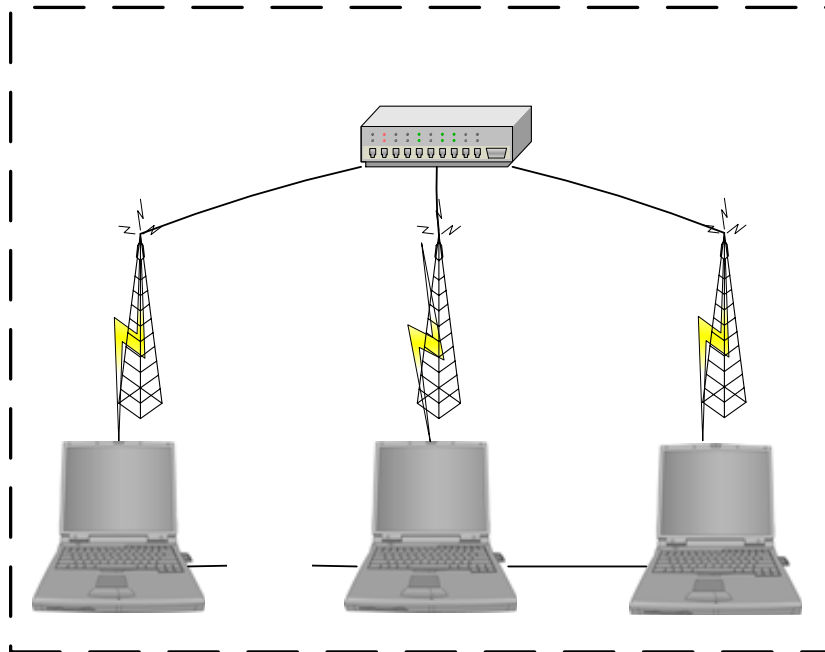



Figura B.4 – Wireless ARP Poisoning: 3 *hosts* na porção sem fio

Nestes ataques, além de conseguir efetuar o ataque de Homen-no-Meio, um eventual atacante pode capturar todo o tráfego sem fio, entre as duas estações, mesmo que estas não estejam necessariamente dentro da mesma área de cobertura.
Na figura anterior, o que se observa é que um ataque que necessitaria ou de uma máquina comprometida em um domínio de *broadcast* ou de acesso físico a dispositivos de rede, podem ser disparados a distância, com equipamentos próprios e de maneira eficaz. Portanto, este tipo de ataque volta a ser uma grande ameaça à segurança das redes sem fio. [FD02]